bitdefender
BUSINESS SOLUTIONS

EXCHANGE

Administrator's guide

bitdefender

BitDefender Security for Exchange
Administrator's guide

Published 2010.05.21

Copyright© 2010 BitDefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of BitDefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of BitDefender, therefore BitDefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. BitDefender provides these links only as a convenience, and the inclusion of the link does not imply that BitDefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Table of Contents

License and Warranty viii

Preface xiii

1. Conventions Used in This Book xiii
   1.1. Typographical Conventions xiii
   1.2. Admonitions xiv
2. The Book Structure xiv
3. Request for Comments xv

Installation ***1***

1. System Requirements **2**

2. Installing BitDefender Security for Exchange **3**

2.1. Fresh Installation 3
2.2. Modifying Existing Installation 6

3. Repairing or Removing BitDefender **7**

3.1. Modify BitDefender 7
3.2. Repair BitDefender 8
3.3. Remove BitDefender 8

Description ***10***

4. Features and Benefits **11**

4.1. Key Benefits 11
4.2. Key Features 13
4.3. BitDefender Advanced Technologies 13
4.4. Services 13

5. Core Modules **15**

5.1. Antivirus 15
5.2. Antispam 16
   5.2.1. Global Filters 17
   5.2.2. Policy Filters 18
5.3. Content Filtering 21
5.4. Attachment Filtering 21

6. How Does It Work? **22**

6.1. SMTP Scanning 22
   6.1.1. Antispam Filtering 22
   6.1.2. Content Filtering 24
   6.1.3. Attachment Filtering 25
   6.1.4. Antivirus Scanning 25

6.2. Mailbox (VSAPI) Scanning 25

Configuration and Management 27

7. Getting Started 28
7.1. Connecting to Another Computer 29
7.2. Changing the Administrative Password 30
7.3. Exporting/Importing Product Settings 31
7.3.1. Exporting Product Settings 31
7.3.2. Importing Product Settings 32

8. Registration and My Account 35
8.1. Step 1/3 - Register BitDefender Security for Exchange 36
8.2. Step 2/3 - Register a BitDefender Account 37
8.3. Step 3/3 - Finish 39

9. Monitoring 40
9.1. Dashboard 41
9.1.1. Important Links 42
9.1.2. Status Area 42
9.1.3. Scan Activity 48
9.1.4. Product Status 49
9.2. Statistics 49
9.2.1. Clearing All Records 52
9.3. Reports 52
9.3.1. Managing Reports 55
9.3.2. Creating Reports 55
9.4. Alerts & Logs 60
9.4.1. Alerts 60
9.4.2. Logs 66
9.4.3. Events 67
9.5. Quarantine 75
9.5.1. Antivirus Quarantine 76
9.5.2. Antispam Quarantine 77
9.5.3. Content Filtering Quarantine 78
9.5.4. Attachment Filtering Quarantine 79
9.5.5. Managing Quarantine 81
9.6. Scheduled Tasks 84
9.6.1. Managing Scheduled Tasks 85
9.6.2. Update Tasks 86
9.6.3. Generate Report Tasks 92
9.6.4. On-demand Scanning Tasks 103

10. SMTP Groups 120
10.1. Managing Groups 121
10.2. Creating Groups 121

10.3. Configuring Groups 121

11. Antivirus 124
11.1. Real-time Antivirus Protection 125
11.1.1. Configuring Advanced Antivirus Settings 126
11.2. Policies 130
11.2.1. Managing Rules 131
11.2.2. Creating Rules 133
11.2.3. Configuring Rules 133
11.3. On-demand Scanning 142
11.3.1. Configuring Scan Settings 143
11.3.2. Viewing Scan Reports 149

12. Antispam 150
12.1. Antispam Filtering 151
12.1.1. Configuring Global Antispam Filters 152
12.2. Policies 159
12.2.1. Managing Rules 159
12.2.2. Creating Rules 160
12.2.3. Configuring Rules 161

13. Content Filtering 174
13.1. Content Filtering 175
13.2. Policies 176
13.2.1. Managing Rules 176
13.2.2. Creating Rules 177
13.2.3. Configuring Rules 178

14. Attachment Filtering 188
14.1. Attachment Filtering 189
14.2. Policies 190
14.2.1. Managing Rules 190
14.2.2. Creating Rules 191
14.2.3. Configuring Rules 192

15. Update 201
15.1. Update 202
15.1.1. Update Information 202
15.1.2. Product Update 203
15.2. Update Settings 204
15.2.1. Configuring Update Schedule 204
15.2.2. Using Update Pushing 205
15.2.3. Configuring Product Updates 206
15.3. Update Locations 207
15.4. Update Notifications 208
15.5. Update Roll Back 210
15.6. Manual Update 211

16. General 213
16.1. Report Virus 213
16.2. Report Incidents 214

Testing BitDefender 216

17. Antivirus Test 217

18. Antispam Test 218

Troubleshooting and Getting Help 219

19. BitDefender Configuration Repair Tool 220

20. BitDefender Support Tool 223

21. Support 225
21.1. Asking for Help 225
21.2. BitDefender Knowledge Base 225
21.3. Contact Information 226
21.3.1. Web Addresses 226
21.3.2. BitDefender Offices 226

License and Warranty

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL THE SOFTWARE. BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT.

These Terms cover BitDefender Corporate Solutions and Services for Companies licensed to you, including related documentation and any update and upgrade of the applications delivered to you under the purchased license or any related service agreement as defined in the documentation and any copy of these items.

This License Agreement is a legal agreement between you (either an individual or a legal person) and BitDefender for use of BitDefender's software product identified above, which includes computer software and services, and may include associated media, printed materials, and "online" or electronic documentation (hereafter designated as "BitDefender"), all of which are protected by international copyright laws and international treaties. By installing, copying or using BitDefender, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not install or use BitDefender.

BitDefender License. BitDefender is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. BitDefender is licensed, not sold.

GRANT OF LICENSE. BitDefender hereby grants you and only you the following non-exclusive, limited, non-transferable and royalty-bearing license to use BitDefender.

APPLICATION SOFTWARE. You may install and use BitDefender, on as many computers as necessary with the limitation imposed by the total number of licensed users. You may make one additional copy for back-up purpose.

SERVER USER LICENSE. This license applies to BitDefender software that provides network services and can be installed on computers that provide network services. You may install this software on as many computers as necessary within the limitation imposed by the total number of users to which these computers provide network services. This limitation refers to the total number of users that has to be less than or equal to the number of users of the license.

DESKTOP USER LICENSE. This license applies to BitDefender software that can be installed on a single computer or on a single operating system (any physical or virtual machine running an operating system) and which does not provide network services

(excepting the case when the desktop computer provides network services by running BitDefender Management Server). Each user may install this software on a single computer or on a single operating system and may make one additional copy for backup on a different device. The number of users allowed is the number of the users of the license.

SUITE LICENSE. This license applies to BitDefender Suites or software bundles. Such Suites or bundles are comprised of:

- server components that can be installed on as many computers or network servers as necessary while retaining the limitation imposed on the total number of client machines established by the license bought
- client components, that can be installed on a single desktop computer or on a single operating system (any physical or virtual machine running an operating system) which does not provide network services (excepting the case when the desktop computer provides network services by running BitDefender Management Server); the number of client machines allowed is less than or equal to the number of client machines for which the Suite License is granted. This limitation refers to the total number of computers or operating systems licensed (any physical or virtual machine running an operating system).

TERM OF LICENSE. The license granted hereunder shall commence on the purchasing date of BitDefender and shall expire at the end of the period for which the license is purchased.

EXPIRATION. The product will cease to perform its functions immediately upon expiration of the license.

UPGRADES. If BitDefender is labeled as an upgrade, you must be properly licensed to use a product identified by BitDefender as being eligible for the upgrade in order to use BitDefender. A BitDefender labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License Agreement. If BitDefender is an upgrade of a component of a package of software programs that you licensed as a single product, BitDefender may be used and transferred only as part of that single product package and may not be separated for use by more than the total number of licensed users. The terms and conditions of this license replace and supersede any previous agreements that may have existed between you and BitDefender regarding the original product or the resulting upgraded product.

COPYRIGHT. All rights, titles and interest in and to BitDefender and all copyright rights in and to BitDefender (including but not limited to any images, photographs, logos, animations, video, audio, music, text, and "applets" incorporated into BitDefender), the accompanying printed materials, and any copies of BitDefender are owned by BitDefender. BitDefender is protected by copyright laws and international treaty provisions. Therefore, you must treat BitDefender like any other copyrighted material. You may not copy the printed materials accompanying BitDefender. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which BitDefender exists. You may not sub-license, rent, sell, lease or share the BitDefender license. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for BitDefender.

LIMITED WARRANTY. BitDefender warrants that the media on which BitDefender is distributed is free from defects for a period of thirty days from the date of delivery of BitDefender to you. Your sole remedy for a breach of this warranty will be that BitDefender , at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for BitDefender. BitDefender does not warrant that BitDefender will be uninterrupted or error free or that the errors will be corrected. BitDefender does not warrant that BitDefender will meet your requirements.

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, BITDEFENDER DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS, ENHANCEMENTS, MAINTENANCE OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) OR SERVICES SUPPLIED BY HIM. BITDEFENDER HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON INTERFERENCE, ACCURACY OF DATA, ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON INFRINGEMENT OF THIRD PARTY RIGHTS BY FILTERING, DISABLING, OR REMOVING SUCH THIRD PARTY'S SOFTWARE, SPYWARE, ADWARE, COOKIES, EMAILS, DOCUMENTS, ADVERTISEMENTS OR THE LIKE, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE.

DISCLAIMER OF DAMAGES. Anyone using, testing, or evaluating BitDefender bears all risk to the quality and performance of BitDefender. In no event shall BitDefender be liable for any damages of any kind, including, without limitation, direct or indirect damages arising out of the use, performance, or delivery of BitDefender, even if BitDefender has been advised of the existence or possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL BITDEFENDER'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR BITDEFENDER. The disclaimers and limitations set forth above will apply regardless of whether you accept to use, evaluate, or test BitDefender.

IMPORTANT NOTICE TO USERS. THIS SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

GENERAL. This Agreement will be governed by the laws of Romania and by international copyright regulations and treaties. The exclusive jurisdiction and venue to adjudicate any dispute arising out of these License Terms shall be of the courts of Romania.

Prices, costs and fees for use of BitDefender are subject to change without prior notice to you.

In the event of invalidity of any provision of this Agreement, the invalidity shall not affect the validity of the remaining portions of this Agreement.

BitDefender and BitDefender logos are trademarks of BitDefender. All other trademarks used in the product or in associated materials are the property of their respective owners.

The license will terminate immediately without notice if you are in breach of any of its terms and conditions. You shall not be entitled to a refund from BitDefender or any resellers of BitDefender as a result of termination. The terms and conditions concerning confidentiality and restrictions on use shall remain in force even after any termination.

BitDefender may revise these Terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed with the revised terms. If any part of these Terms is found void and unenforceable, it will not affect the validity of rest of the Terms, which shall remain valid and enforceable.

In case of controversy or inconsistency between translations of these Terms to other languages, the English version issued by BitDefender shall prevail.

Contact BitDefender, at 24 Preciziei Street, West Gate Park, Building H2, ground floor, Sector 6, Bucharest, Romania, or at Tel No: 40-21-206.34.70 or Fax: 40-21-264.17.99, e-mail address: office@bitdefender.com.

Preface

This guide is intended to all network administrators who have chosen BitDefender Security for Exchange as a security solution for their company's Microsoft Exchange servers. The information presented in this book is suitable not only for computer literates, it is accessible to everyone who is able to work under Windows.

This book will describe for you BitDefender Security for Exchange, will guide you through the installation process, will teach you how to configure it. You will find out how to use BitDefender Security for Exchange, how to update, test and customize it. You will learn how to get best from BitDefender.

We wish you a pleasant and useful lecture.

1. Conventions Used in This Book

1.1. Typographical Conventions

Several text styles are used in the book for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	*Description*
`sample syntax`	Syntax samples are printed with `monospaced` characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on HTTP or FTP servers.
sales@bitdefender.com	E-mail messages are inserted in the text for contact information.
“Preface” (p. xiii)	This is an internal link, towards some location inside the document.
`filename`	File and directories are printed using `monospaced` font.
option	All the product options are printed using **strong** characters.
`sample code listing`	The code listing is printed with `monospaced` characters.

1.2. Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.

Note
The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.

Important
This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.

Warning
This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

2. The Book Structure

The book consists of 5 parts, containing the major topics: Installation, Description, Configuration and Management, Testing BitDefender, and Troubleshooting and Getting Help.

Installation. Step by step instructions for installing BitDefender on a workstation. This is a comprehensive tutorial on installing BitDefender Security for Exchange. Starting with the prerequisites for a successfully installation, you are guided through the whole installation process. Finally, the removing procedure is described in case you need to uninstall BitDefender.

Description. The features and functionality of BitDefender Security for Exchange are presented to you.

Configuration and Management. Description of basic administration and maintenance of BitDefender. The chapters explain in detail all options of BitDefender Security for Exchange, how to register the product, how to configure it, how to monitor its activity and how to perform the updates.

Testing BitDefender. Presents two standard testing methods that you can use to check the antivirus and antispam components of BitDefender.

Troubleshooting and Getting Help. Where to look and where to ask for help if something unexpected appears.

3. Request for Comments

We invite you to help us improve the book. We have tested and verified all of the information to the best of our ability. Please write to tell us about any flaws you find in this book or how you think it could be improved, to help us provide you with the best documentation possible.

Let us know by sending an e-mail to documentation@bitdefender.com.

Important

Please write all of your documentation-related e-mails in English so that we can process them efficiently.

Installation

1. System Requirements

Before installing the product, make sure that your system meets the following minimum system requirements:

- **Operating system:**
  - Windows 2000 with Service Pack 4 and Update Rollup 1
  - Windows Server 2003 with Service Pack 1
  - Windows Server 2008
- Exchange 2003 Standard or Enterprise or
- Exchange 2000 Standard or Enterprise with Service Pack 3
- Internet Explorer 6 or higher
- **Hardware:**
  - **64-bits**
    - Any 64-bit Windows station (Intel or AMD)
    - Minimum 1 GB of free space on the hard drive
  - **32-bit**
    - Minimum Processor - Pentium III 500 MHz
    - Minimum 256 megabytes (MB) of RAM, 512 MB recommended
    - Minimum 1 GB of free space on the hard drive

2. Installing BitDefender Security for Exchange

In order to install BitDefender Security for Exchange, you need an installation file or an installation CD that contains the installation package. The installation file comes under different names, depending on the BitDefender business products it contains. You can download the installation file from www.bitdefender.com.

There are two versions of the installation package:

- **32-bit** - use this version if you want to install BitDefender Security for Exchange on a 32-bit computer.
- **64-bit** - use this version if you want to install BitDefender Security for Exchange on a 64-bit computer.

The installation package contains other BitDefender Security for Windows Servers products besides BitDefender Security for Exchange. You should install all the products you want to use at the same time. If you install only BitDefender Security for Exchange, you will then need to modify the existing installation whenever other BitDefender products are installed at a later time. As a result of this action, some files may need to be replaced, which may temporarily interfere with the operation of the existing installed products.

Depending on whether or not you already have BitDefender products installed on the computer, there are two ways to install BitDefender Security for Exchange:

- **Fresh installation** - no other product from the installation package is installed on the computer.
- **Modifying an existing installation** - at least one other product from the installation package is already installed on the computer.

2.1. Fresh Installation

To begin a fresh installation, locate the setup file and double-click it. A wizard will appear and you must follow its steps to complete installation. Detailed information is provided for each situation. Follow the instructions suited for your current situation.

Before launching the setup wizard, BitDefender will check for newer versions of the installation package. If a newer version is available, you will be prompted to download it. Click **Yes** to download the newer version or **No** to continue installing the version then available in the setup file.

BitDefender will also check if BitDefender Security for Exchange is already installed on the local computer. If the same version as the one in the setup file is installed, you will have to modify the existing configuration. If an older version is installed, the installation process will continue as it should, with the only difference that the already installed products will be re-installed (upgraded) by default.

Installation Steps

Follow these steps to install BitDefender Security for Exchange:

1. Click **Next** to continue or click **Cancel** if you want to quit installation.

Note

After you click **Next**, BitDefender will check if your system meets the minimum requirements for the product and will inform you of any issues that might require your attention before installation can continue.

2. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.

   Note
   If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

3. You can see the list of all BitDefender products designed for Windows-based servers available in the installation package.

   Select BitDefender Security for Exchange, click the corresponding **arrow** and then click **Will be installed on local hard drive** on the shortcut menu.

   The default installation folder is displayed on the lower part of the window. To select a different installation folder, click **Browse**, locate the folder and then click **OK** to set the location.

   Note
   You can also install other BitDefender products for Windows-based servers. Select them as shown before. The items marked with a red cross will not be installed.

   Click **Next**.

   Note
   If BitDefender does not detect a Microsoft Exchange Server installed on the local computer, an error message will appear and the installation process will be cancelled. Click **OK&Finish** to exit the wizard.

4. Click **Next**.
5. BitDefender Security for Exchange contains an incident management module that allows creating incident reports during product crashes. By agreeing to send the incident reports to the BitDefender Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs. The reports will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

   To send incident reports to the BitDefender Lab, select **I agree to submit incident reports to the BitDefender Lab** and specify your e-mail address.

   Click **Next**.

6. If you do not want the readme file to be opened at the end of the installation, clear the **View Readme file** check box. Click **Install** in order to begin the installation of the product.

Note
BitDefender will automatically detect your version of Microsoft Exchange Server.

7. Click **Finish** to complete product installation.

Note
You may be asked to restart your system so that the setup wizard can complete the installation process.

2.2. Modifying Existing Installation

In order to install BitDefender Security for Exchange when one or more BitDefender Security for Windows Servers products are already installed on the computer, you need to follow these steps:

1. Follow the next path from the Windows Start Menu: **Start** → **Programs** → **BitDefender Security for Windows Servers** → **Modify, Repair or Uninstall**.

Note
Alternatively, you can double click the BitDefender Security for Windows Servers setup file.

   A welcome window will appear, click **Next** to begin.
2. Select **Modify**.
3. You have now reached Step 3 of the "*Fresh Installation*" (p. 3) wizard. Follow steps 3 through 7 to complete the installation.

3. Repairing or Removing BitDefender

If you want to modify, repair or remove **BitDefender**, follow this path from the Windows start menu: **Start → Programs → BitDefender Security for Windows Servers → Modify, Repair or Uninstall**.

You will be requested to confirm your choice by clicking **Next**. A new window will appear where you can select:

- **Modify** - to add new BitDefender products for Windows-based servers or to remove currently installed products.
- **Repair** - to re-install BitDefender Security for Exchange.
- **Remove** - to remove all installed components.

BitDefender Security for Windows Servers Setup
Repair or Remove BitDefender
Select the operation you wish to perform.
Modify
Allows users to change the way features are installed.
Repair
Repairs errors in the most recent installation state - fixes missing or corrupt files, shortcuts and registry entries.
Remove
Removes BitDefender Security for Windows Servers from your computer.
< Back
Next >
Cancel

Modify, Repair or Remove BitDefender

3.1. Modify BitDefender

The BitDefender Security for Exchange installation package is part of a bigger package that contains all available BitDefender Security for Windows Servers products.

If you choose **Modify**, a new window will appear from which you can select individual BitDefender products for installation or removal.

You should install all the products you want to use at the same time.

To install a product, click the corresponding **arrow** and then select **Will be installed on local hard drive** on the shortcut menu.

To remove a product, click the corresponding **arrow** and then select **Entire feature will be unavailable** on the shortcut menu.

3.2. Repair BitDefender

If BitDefender Security for Exchange starts to perform unexpectedly, you can repair it in order to restore its functionality. The repair process consists in completely re-installing the product.

Important

Before repairing the product, we recommend you to export the product settings so that you can reload them after the repairing process is completed. For more information, please refer to "*Exporting/Importing Product Settings*" (p. 31).

If you choose **Repair**, a new window will appear. Click **Repair** to start the process.

Important

During the repair process all BitDefender products installed on the computer will temporarily cease to function.

3.3. Remove BitDefender

If you want to uninstall all BitDefender products, choose **Remove**.

Note

We recommend that you choose **Remove** for a clean re-installation.

If you choose to remove BitDefender, a new window will appear. Click **Remove** to start unsinstalling BitDefender from your computer.

Important

This will remove all BitDefender products from your computer. If you have additional BitDefender products installed and only wish to remove BitDefender Security for Exchange, please use the Modify option.

After the removal process is over, we recommend that you delete the `BitDefender` folder from `Program Files`.

An error occurred while removing BitDefender

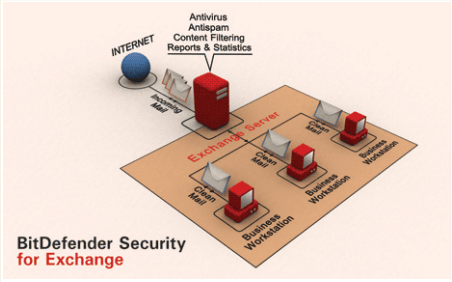
If an error has occurred while removing BitDefender, the removal process will be aborted and a new window will appear. Click **Run UninstallTool** to make sure that BitDefender has been completely removed. The uninstall tool will remove all the files and registry keys that were not removed during the automatic removal process.

Description

4. Features and Benefits

Comprehensive protection for Exchange Servers

BitDefender Security for Exchange provides antivirus, antispyware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the MS Exchange Server, to create a malware free messaging environment. It protects Exchange servers against the latest, most sophisticated malware and against attempts to steal users' confidential and valuable data.



Comprehensive protection for Exchange Servers

4.1. Key Benefits

- **Email Protection against malware**
  - Fights e-mail-borne malware by filtering and blocking messages that carry a virus, spyware, trojan, backdoor or other potentially dangerous active codes
  - Scans e-mail messages at the point they enter/leave the server so that the messaging environment is free from malware at all times
  - Extends the malware protection span by keeping the external recipients of the filtered e-mail (customers, partners, friends) safe as well
  - Offers anti-phishing protection by proactively detecting forged messages intended trick their recipient into disclosing confidential data
  - Matches e-mails to a particular IP address so that messages with spoofed headers cannot pass the White List filter anymore
- **Increased business productivity**
  - Reduces mail traffic and saves network resources due to its extensive antimalware protection capabilities

- Through its optimized scanning process, increases mail delivery speed and reduces server workload
- Improves the IT manager's productivity and prevents the loss of confidential information by filtering all mail passing through the Exchange server based on content (subject line, sender, recipient) and attachment and the criteria defined for the existing user groups.
- Provides a highly efficient multi-layered antispam protection system which:
  - Reduces mail traffic by accurately classifying messages as spam, phishing or legitimate
  - Blocks unsolicited mail based on connection filters such as the Allow/Deny IP List and Sender Black List, on the Bayesian and the Real-time Blackhole List (RBL) filters.
  - Allows configuring antispam filter sensitivity by setting very demanding or relaxed thresholds for each user group
  - Automatically redirects spam mails to your Exchange Junk Folder
- Provides WBL (White List / Black List) support, allowing you to set a list of trusted and untrusted addresses based on which to respectively "always accept" or "always reject" mail

- **Increased usability**
  - Allows you to filter mail traffic in a more flexible manner through the use of antivirus, antispam, content and attachment filtering policies for different groups or users
  - Generates detailed statistics and reports based on a comprehensive database related to the product's activity
  - Allows you to remotely configure server protection by simply installing the management console on one computer inside the network
  - Instantaneously sends detailed warning messages to the network security and management staff if a virus is detected
  - Can isolate dangerous or restricted mails going through the antivirus, antispam, content and attachment filtering modules in a quarantine zone where you can deal with them at will
- **Centralized management support**

  BitDefender Management Server allows centrally managing most of the BitDefender business solutions installed on network computers, including BitDefender Security for Exchange. This type of integration allows you to use the Management Server console to get centralized access to:
  - Configuration settings for BitDefender Security for Exchange
  - Critical event information such as update-related events, configuration warnings, license expiration

- Easy-to-interpret statistics and reports based on the information received from BitDefender Security for Exchange

4.2. Key Features

- Certified antivirus engines
- Proactive heuristic protection against zero-day threats
- Multiple layers of anti-spam filtering
- Content and attachment filtering
- Antispyware and antiphishing protection
- Centralized management software compatibility

4.3. BitDefender Advanced Technologies

B-HAVE. BitDefender Security for Exchange includes B-HAVE, a patent pending technology which analyzes the behavior of potentially malicious codes, inside a virtual computer, eliminating false positives and significantly increasing detection rates for new and unknown malware.

Image Spam Filter. BitDefender offers a more accurate image filter which, instead of analyzing the text within image spam messages, learns the common characteristics of those images in point of color content and proportions. The result: less false positives and lower spam traffic.

NeuNet Filter. To better deal with new spam, the BitDefender Lab has created NeuNet, a powerful antispam filter. Inside the Antispam Lab, NeuNet is pre-trained on a series of spam messages so that it learns to recognize new spam by perceiving its similarities with the messages it has already examined.

Certified Antivirus Engines. BitDefender's award winning scan engines featuring the B-HAVE technology have been recognized by ICSA Labs, Virus Bulletin and Checkmark to provide the most proactive antivirus protection available.

4.4. Services

Advanced Update System. For permanent server protection, the product receives the latest updates and patches based on four configurable technologies: on-demand, scheduled, automatic and pushed.

Upgrades. Registered users benefit from free upgrades to any new version of the product during the license period. Special price offers are also available to returning customers.

Free 24/7 Professional Technical Support. Certified representatives provide BitDefender business customers with free permanent support online, by telephone or e-mail. This is supplemented by an online database with answers to Frequently Asked Questions and fixes for common issues.

5. Core Modules

The core functionalities of BitDefender Security for Exchange are defined by 4 modules: **Antivirus**, **Antispam**, **Content Filtering** and **Attachment Filtering**.

5.1. Antivirus

Basically, there are two kinds of antivirus scanning:

- Antivirus scanning at SMTP (Simple Mail Transfer Protocol) level
- Antivirus scanning at mailbox, or VSAPI (Virus Scanning Application Program), level

Antivirus scanning at SMTP level. BitDefender scans the SMTP mail entering or leaving the Exchange server for viruses, spyware and other malware. Different scanning policies can be defined for users and user groups. These policies include sets of rules specifying the antivirus scanning settings and the actions to be taken on infected messages depending on the groups the sender and the recipients belong to.

Antivirus scanning at mailbox (VSAPI) level. BitDefender protects the Exchange server from viruses, spyware and other malware by scanning the messages and the files in users' mailboxes and server folders upon clients' request. The MS Exchange mail server was designed with a low level interface, VSAPI, intended to offer antivirus scanning support. This interface also allows scanning messages with multiple recipients once, before delivery, instead of several times, for each mail recipient separately. BitDefender deeply integrates with this interface.

The antivirus scanning at VSAPI level can be done through three additional scanning methods, intended to optimize the overall scanning process: background, proactive or transport scanning.

- The purpose of background scanning is to scan all messages stored in the Exchange databases (mailboxes and public folders). When an object having been checked through background scanning is requested, it will not be scanned again unless a virus signature update has been performed in the meantime.

  Although background scanning is performed at low priority, the process takes up system resources because databases are re-scanned after each update and updates are performed often.

Note

By default background scanning is disabled. You should enable it only as a second layer of protection when you want to check all your databases and make sure they are clean.

- Proactive scanning allows scanning messages before they are actually accessed. When a message is submitted to the Store, it is placed in the global scanning queue and assigned a low priority. If and when threads are available in the thread pool and no high priority message remains to be scanned, each message in the global scanning queue is submitted for scanning. On the other hand, if a message in the global scanning queue is requested by a client, it is assigned a high priority and it is removed from the low priority list.

  Proactive scanning optimizes the overall scanning process because the messages having undergone proactive scanning are not scanned again when accessed (unless the virus stamp has changed in the meantime).

  Note

  By default, proactive scanning is enabled.

- Transport scanning prevents infected messages from entering Exchange mailboxes. After entering the Exchange store, the messages are scanned before being resubmitted to the transport engine which delivers them to their destination. Messages are then scanned again on the back-end server.

  Note

  By default, transport scanning is enabled.

In order to configure proactive, background and transport scanning, open the management console, go to the **Antivirus** module, Real time tab and click **Advanced**. For more information, please refer to "*Configuring Advanced Antivirus Settings*" (p. 126).

5.2. Antispam

BitDefender Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox.

Different filtering policies can be defined for users and user groups. The rules are those that specify which filters to use to analyze the message and the actions to take on spam, based on the groups to which the sender and the recipients belong.

The Antispam filters are grouped into two categories:

- **Global filters** - configurable filters meant to filter all incoming mail traffic, regardless of the policies set.
- **Policy filters** - filters applied to the incoming mail traffic according to the specified policies.

5.2.1. Global Filters

There are 4 global filters: Allow / Deny IP List, Sender Black List, IP Match and Real-time Blackhole List.

Note

These filters must be configured globally by the administrator. In order to configure them, go to the **Antispam** module, Antispam section and click **Global Filters**. For more details, please refer to "*Configuring Global Antispam Filters*" (p. 152).

Allow / Deny IP List

The Allow / Deny IP List enables the administrator to specify IP addresses which are denied access to the server. All incoming connections from addresses that appear on the Deny IP List are dropped, provided that such addresses do not appear on the Allow IP List. The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Sender Black List

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

IP Match

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match.

If a message appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), BitDefender checks to see if the IP

address of the sender matches one of the IP addresses provided for the specified domain. If the domain address of the sender matches an associated IP address, the message is considered legitimate and antispam filtering stops. Otherwise, the message is considered SPAM and the connection is dropped.

Real-time Blackhole List

The Real-time Blackhole List (RBL) filter allows checking the mail server from which a message is sent against the RBL servers configured by the administrator. It uses the DNSBL protocol and RBL servers to filter spam based on mail servers' reputation as spam senders.

The mail server address is extracted from the e-mail header and its validity is checked. If the address belongs to a private class (`10.0.0.0`, `172.16.0.0` to `172.31.0.0` or `192.168.0.0` to `192.168.255.0`) or it is not relevant, it will be ignored.

A DNS check is performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com` is the RBL server. If the DNS replies that the domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score ranges between 0 and 100, according to the configured server confidence (trust level).

The query is performed for every RBL server in the list and the score returned by each one is added to the intermediate score. When the score has reached `100`, no more queries are performed.

If the RBL filter score is 100 or higher, the message is considered SPAM and the specified action is taken. Otherwise, a spam score is computed from the RBL filter score and added to the global spam score of the message.

Note
The RBL filter can be deactivated under certain policies.

5.2.2. Policy Filters

There are 8 policy filters: White List / Black List, Block sexually explicit content, Charset filter, URL filter, Image filter, Bayesian filter, Pre-trained Bayesian filter and NeuNet (Heuristic) filter.

Note

These filters can be enabled and configured by the administrator separately for each rule. In order to configure them, go to the **Antispam** module, Policies section and set the appropriate rules. For more details, please refer to "*Creating Rules*" (p. 160).

White List / Black List

Most people communicate regularly with a group of people or even receive messages from companies or organizations in the same domain. By using the White List / Black List filter, the administrator can set a list of trusted and untrusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

Note

We recommend that you add the trusted addresses to the White List. BitDefender does not block messages coming from the addresses on the list; therefore, adding them helps ensure that legitimate messages get through.

The filter is highly flexibile as it can be configured separately for different groups of users. Note that the lists must be configured for each rule in order to apply the filter to the corresponding incoming mail traffic.

Block Sexually Explicit Content

Starting May 19, 2004, spam that contains sexually oriented material must include the warning `SEXUALLY-EXPLICIT:` in the subject line or face fines for violations of federal law.

This filter detects messages marked as `SEXUALLY-EXPLICIT:` in the subject line and tags them as SPAM.

Charset Filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

URL Filter

Almost all spam messages include links to various web locations. These locations usually contain more advertising and the possibility to buy things, and, sometimes, they are used for phishing.

BitDefender maintains a database of such links. The URL filter checks every URL link in a message against its database. If a match is made, the message is tagged as SPAM.

Image Filter

Since avoiding heuristic filter detection has become quite a challenge, images are increasingly used in spam messages. Many spam messages contain either a single spam image or a spam image and a random text meant to deceive the heuristic filter.

The Image filter deals with image spam. It compares the image from a message with those from the BitDefender database. In case of a match, the message is tagged as SPAM.

Bayesian Filter

The Bayesian filter is the trainable component of the Antispam module. It constantly collects statistical information about server-specific spam and legitimate messages provided by the administrator and it analyzes messages according to this information

This information refers to the rate at which specific words appear in messages classified SPAM as compared to those declared NON-SPAM. This means, for example, that if a certain four-letter word is seen to appear more often in SPAM, it will be naturally presumed that it is very likely for the next incoming message including this word to actually be SPAM. All relevant words within a message are taken into account. By synthesizing the statistical information, the overall probability for the whole message to be SPAM is computed and a SPAM score is added to the message.

Pre-trained Bayesian Filter

While the Bayesian filter is trained on server-specific messages, this filter is pretrained by the BitDefender Antispam Lab on our own database of spam and legitimate messages and updated periodically.

NeuNet (Heuristic) Filter

The NeuNet (Heuristic) filter performs a set of tests on all message components, (i.e. not only the header but also the message body in either HTML or text format), looking for words, phrases, links or other characteristics of SPAM. Based on the results of the analysis, it adds a SPAM score to the message.

5.3. Content Filtering

Content Filtering checks messages to see if the subject, the sender's or the recipient(s)' address contain certain specified strings. If a defined string matches one of these mail headers, the message is detected and the specified action is taken. Both incoming and outgoing SMTP mail is verified.

Different filtering policies can be defined for users and user groups. The rules are those that specify the filtering settings and the actions to be taken on the messages that match the rule, based on the groups to which the sender and the recipients belong.

5.4. Attachment Filtering

Attachment Filtering checks mail attachments to see if their name matches certain patterns, if they have a different extension than those specified or if they exceed a certain size limit. In any of these cases, the message containing the respective attachment is detected and the specified action is taken. Both incoming and outgoing SMTP mail is verified.

The filter will check file headers and correctly identify the attachment file type when scanning for restrictred extensions. This means an extension can not be simply renamed to bypass attachment filtering policies.

Different filtering policies can be defined for users and user groups. The rules are those that specify the filtering settings and the actions to be taken on the messages that match the rule, based on the groups to which the sender and the recipients belong.

6. How Does It Work?

BitDefender Security for Exchange scans e-mail messages both at SMTP (Simple Mail Transfer Protocol) level and at mailbox, or VSAPI (Virus Scanning Application Program), level.

E-mail messages entering or leaving the Exchange server are scanned at SMTP level. Inside the Exchange server, e-mail messages entering or leaving the users' mailboxes are scanned at VSAPI level.

6.1. SMTP Scanning

When working at SMTP level, BitDefender checks mail using antispam, content and attachment filtering, and antivirus scanning. This keeps clients' Inboxes free of spam, phishing attempts, viruses and spyware as well as other unwanted content. Moreover, using content and attachment filtering on outgoing mail protects your company against the theft of confidential information.

Let's consider that all the filters and engines are enabled and see how BitDefender filters the mail traffic. A message is verified, in the following order, by:

1. Antispam Filtering (only incoming SMTP mail)
2. Content Filtering
3. Attachment Filtering
4. Antivirus Scanning

6.1.1. Antispam Filtering

The Antispam module will check the message first. Antispam filtering works at both connection and content level to ensure efficient protection against spammers and less traffic on the server.

Note
For detailed information about the Antispam filters, check the description of the Antispam Module.

Connection Level

When an attempt is made to establish a connection, the message is checked against the **Allow / Deny IP List**. If there is a match, the connection is dropped.

Otherwise, the message is checked against the global **Sender Black List**. If the filter finds a match, the connection is dropped.

Content Level

If the message passes connection level filters, it is unpacked and filtered at content level.

First, the message is checked against the **IP Match** filter. If a match is found, there are two possibilities:

- the message is considered legitimate and antispam filtering stops.
- the connection is dropped.

If the message does not match the IP Match filtering criteria, it is then checked based on a specific **antispam filtering group policy**.

The message is checked against the antispam filtering rules, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the options specified by that rule.

- If the action set for the rule is **Do not scan**, the antispam filtering stops.
- If the action set for the rule is **Scan**, several antispam filters will take over the message in the following order:
  1. **G-Tube.** If the message matches the G-Tube test, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  2. **White List / Black List Filter.** If a match is found against the White List, the filtered message is considered legitimate and the antispam filtering stops. If a match is found against the Black List, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
  3. **Real-time Blackhole List (RBL).** The filter analyzes the message and, if matches are found, modifies its SPAM score. If the SPAM score exceeds a certain value, the message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.

4. **"Block sexually explicit content" Filter.** If the message matches the filtering rule, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
5. **Charset Filter.** If the message matches the filtering rule, it is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
6. **URL Filter.** If a match is found against the filter's database, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
7. **Image Filter.** If a match is found against the filter's database, the filtered message is considered SPAM, the antispam filtering stops and the specified action is taken on the message.
8. **Bayesian Filter.** The filter analyzes the message and modifies its SPAM score.
9. **Pre-trained Bayesian Filter.** The filter analyzes the message and modifies its SPAM score.
10. **NeuNet(heuristic) Filter.** The filter analyzes the message and modifies its SPAM score.

After the last filter checks the message, the SPAM score is compared to the threshold level specified for the rule that is applied. If the final SPAM score exceeds the threshold level, then the message is considered SPAM and the specified action is taken. Otherwise, the message is allowed to pass and BitDefender adds scan information to the e-mail header.

6.1.2. Content Filtering

If the message is not deleted during antispam filtering, it is then verified according to a specific **content filtering group policy**.

The message is checked against the content filtering rules, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the options specified by that rule.

- If the filtering option set for the rule is **Do not scan**, the message is not processed using content filtering.
- If the filtering option set for the rule is **Scan**, the message is checked according to the content filtering options specified by the rule. If the message matches the rule, the content filtering stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass without any action taken.

6.1.3. Attachment Filtering

If the message is not deleted during content filtering, then the mail attachments, if any, are verified according to a specific **attachment filtering group policy**.

The message is checked against the attachment filtering rules, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the options specified by that rule.

- If the option set for the rule is **Do not scan**, the message is not processed using attachment filtering.
- If the filtering option set for the rule is **Scan**, the message is checked according to the attachment filtering options specified by the rule. If the message matches the rule, the attachment filtering stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass without any action taken.

6.1.4. Antivirus Scanning

If the message is not deleted during attachment filtering, it is then verified according to a specific **antivirus scanning group policy**.

The message is checked against the antivirus scanning filtering rules corresponding to policies, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the options specified by that rule.

- If the filtering option set for the rule is **Do not scan**, the message is not scanned for malware.
- If the scan option set for the rule is **Scan**, the message is checked according to the scanning options specified by the rule. If the message is found infected, the scanning stops and the specified actions are taken on the message. Otherwise, the message is allowed to pass and BitDefender adds scan information to the e-mail header and, optionally, to the message footer.

6.2. Mailbox (VSAPI) Scanning

When working at VSAPI level, BitDefender Security for Exchange can perform only real-time and on-deman antivirus scanning. The messages placed into mailboxes and public folders are intercepted by the VSAPI interface upon clients' request and scanned

by BitDefender. The scanning is performed according to the options specified by the default antivirus rule.

Real-time VSAPI scanning can also be done through three additional methods, intended to optimize the overall scanning process: background, proactive or transport scanning.

This is how scanning works:

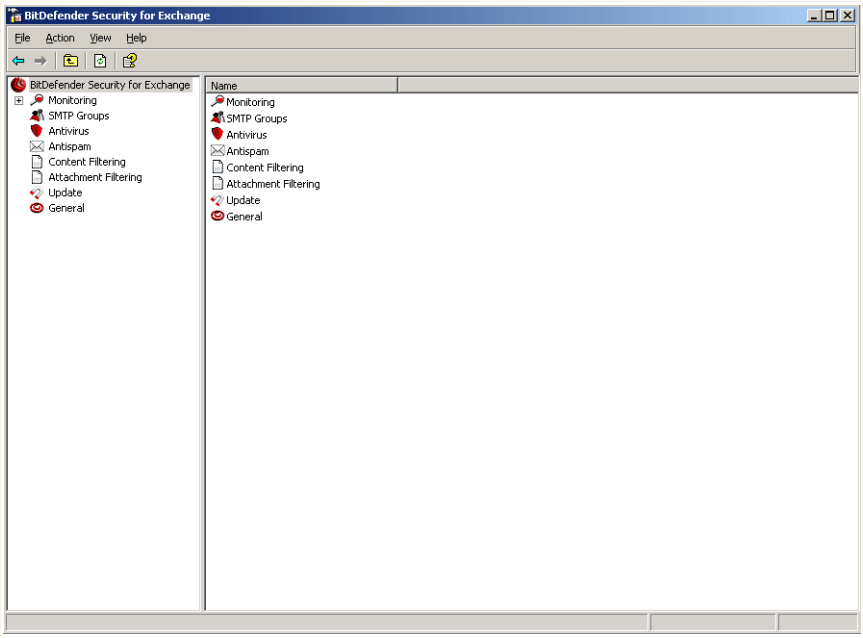
- If the message was checked through proactive or background scanning and no update has been performed in the meantime, the message will be delivered without being scanned again.
- If the message was checked through proactive, transport or background scanning but an update has been performed in the meantime, the message will be scanned again.

Configuration and Management

7. Getting Started

BitDefender Security for Exchange can be configured and managed through a centralized, MMC-based management console. The management console provides access to all features and settings of BitDefender Security for Exchange.

To access the management console, use the Windows Start menu, by following the path **Start → Programs → BitDefender Security for Windows Servers → BitDefender Security for Exchange**.



Management Console

On the left side of the management console you can see the tree menu:

- Monitoring - displays the dashboard. The dashboard provides you with useful information on the status of BitDefender Security for Exchange and helps you easily solve the issues that require your attention.

- Statistics - offers real-time statistical information regarding the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules.
- Reports - allows you to create customized reports on product activity.
- Alerts & Logs - allows configuring the logging options and sending alerts about the events that occur during product operation, such as an update error or an infected file detected.
- Quarantine - stores detected files, grouped into four categories (Antivirus, Antispam, Content Filtering, Attachment Filtering).
- Scheduled Tasks - allows creating scheduled tasks through an intuitive wizard. You can schedule updates, on-demand scanning processes and reports to be generated.

- SMTP Groups - provides group management. By organizing users into groups, you can apply different scanning and filtering policies for different user categories.
- Antivirus - this is where you can configure the **Antivirus** module.
- Antispam - this is where you can configure the **Antispam** module.
- Content Filtering - this is where you can configure the **Content Filtering** module.
- Attachment Filtering - this is where you can configure the **Attachment Filtering** module.
- Update - this is where you can configure the **Update** module and install new updates when they are available.
- General - provides access to the following sections:
  - Report Virus - allows configuring BitDefender to automatically report found viruses and spam to the BitDefender Lab.
  - Report Incidents - allows configuring BitDefender to automatically report operation malfunctions to the BitDefender Lab.

Whenever you need help, simply right click an item in the right side menu and click **Help** in the contextual menu that appears to open the help file. Contextual help is available for each window. Click ? to open it.

7.1. Connecting to Another Computer

The management console allows you to remotely manage other BitDefender Security for Exchange products.

Important
To remotely manage a BitDefender Security for Exchange product, you must first set an administrative password for the respective product.

To connect to a BitDefender Security for Exchange product installed on a remote computer, follow these steps:

1. Right-click **BitDefender Security for Exchange** in the tree menu.
2. From the contextual menu, select **Connect to another computer**. A new window will appear.

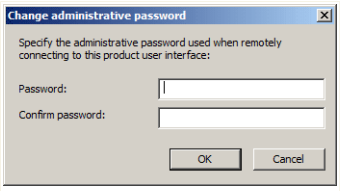
Connect to another computer

3. In the **Connect to computer** field, type the IP address or the name of the remote computer.
4. In the **Password** field, type the administrative password of the respective product.
5. Click **OK**

7.2. Changing the Administrative Password

In order to remotely manage BitDefender Security for Exchange, you must set an administrative password. To set or change the administrative password, follow these steps:

1. Right-click **BitDefender Security for Exchange** in the tree menu.
2. From the contextual menu, select **Change administrative password**. A new window will appear.



Change administrative password

3. In the **Password** field, type the desired administrative password.
4. In the **Confirm password** field, type the password again.
5. Click **OK**

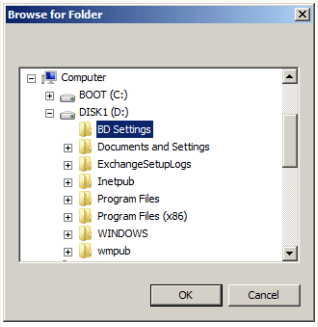
7.3. Exporting/Importing Product Settings

You can export and import the product settings. This helps you easily configure other BitDefender Security for Exchange products within the network and restore configured settings in case you repair or reinstall the product.

7.3.1. Exporting Product Settings

To export the current product settings, follow these steps:

1. Right-click **BitDefender Security for Exchange** in the tree menu.
2. From the contextual menu, select **Export product settings**.



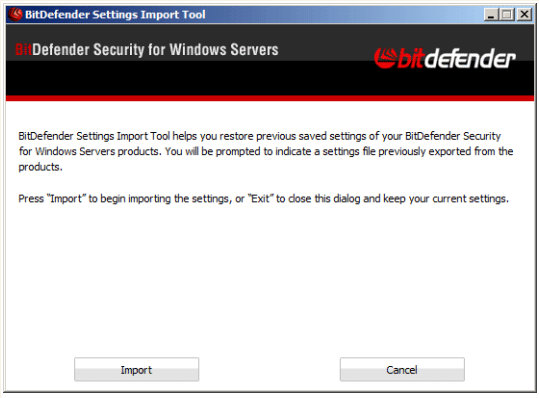
Import Tool

3. Select the folder where to save the product settings and click **OK**.

7.3.2. Importing Product Settings

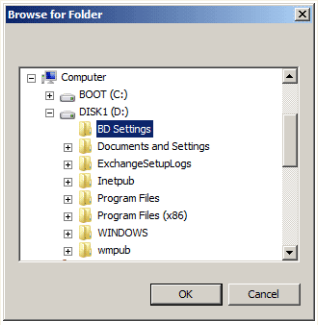
To import previously saved product settings, follow these steps:

1. Right-click **BitDefender Security for Exchange** in the tree menu.
2. From the contextual menu, select **Import product settings** to open the Import Tool.


BitDefender Settings Import Tool
BitDefender Security for Windows Servers
bitdefender
BitDefender Settings Import Tool helps you restore previous saved settings of your BitDefender Security for Windows Servers products. You will be prompted to indicate a settings file previously exported from the products.
Press "Import" to begin importing the settings, or "Exit" to close this dialog and keep your current settings.
Import
Cancel

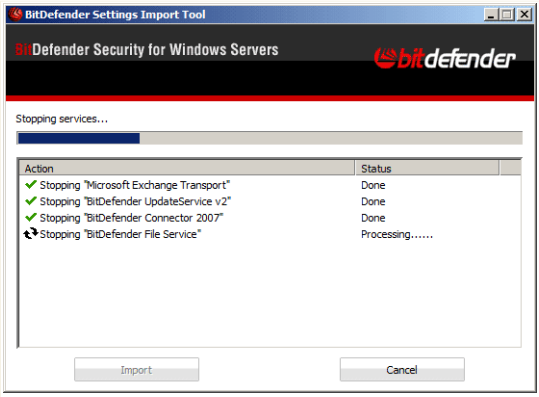
Import Tool

3. Click **Import**. A new window will appear.



Import Tool

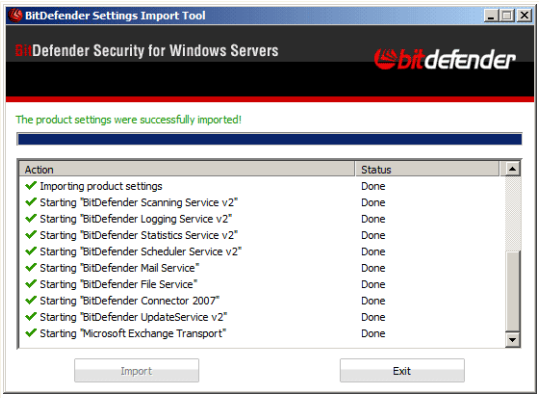
4. Select the folder where the product settings were saved and click **OK** to import them.
5. Wait until the Import Tool completes the importing process.



Importing Settings

The Import Tool first stops the Microsoft Exchange Transport service, the Microsoft Information Store and the BitDefender Security for Exchange services. Then, it imports the product settings from the selected folder. Finally, the Import Tool restarts the processes previously stopped.

6. The Import Tool informs you when the settings have been successfully imported.



Finish

Click **Exit** to close the window.

8. Registration and My Account

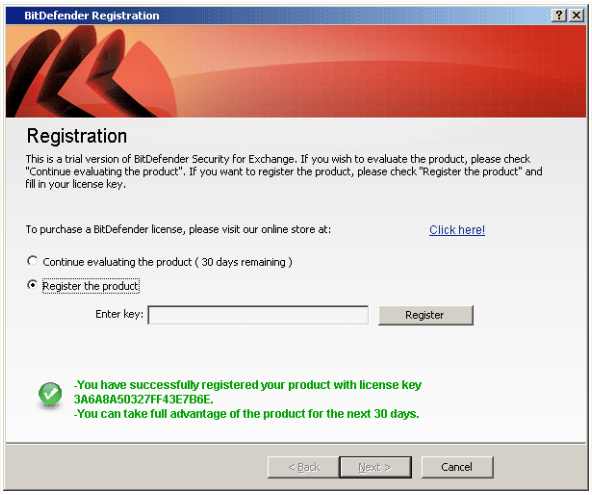
BitDefender Security for Exchange comes with a 30-day trial period. If you decide that BitDefender Security for Exchange is the best choice for your organization, proceed to register its full version. You should also register a BitDefender account in order to benefit from free BitDefender technical support and other free services.

Go to **Monitoring** in the tree menu to perform the product and account registration.

- Click **Register** to register BitDefender Security for Exchange, change the license key, create or sign in to your account or see how many days are left until the licensing period expires.
- Click **My account** if you only want to register or sign in to a BitDefender account.

Note
If BitDefender Security for Exchange is under the management of BitDefender Management Server, the product and account registration are performed from the management console of BitDefender Management Server.

8.1. Step 1/3 - Register BitDefender Security for Exchange


BitDefender Registration
Registration
This is a trial version of BitDefender Security for Exchange. If you wish to evaluate the product, please check "Continue evaluating the product". If you want to register the product, please check "Register the product" and fill in your license key.
To purchase a BitDefender license, please visit our online store at:
Click here!
Continue evaluating the product (30 days remaining)
Register the product
Enter key:
Register
-You have successfully registered your product with license key 3A6A8A50327FF43E7B6E.
-You can take full advantage of the product for the next 30 days.
< Back
Next >
Cancel

Registration

If you do not have a BitDefender license, click the provided link to go to the BitDefender online store and purchase a license key.

To register BitDefender Security for Exchange, select **Register the product**, type the license key in the **Enter key** field and click the **Register** button.

If the trial period has not expired and you want to continue evaluating the product, select **Continue evaluating the product**. You can see the current license key and when it expires.

Click **Next** to continue.

Note

If the provided license key is not valid, you will be prompted to provide another license key.

8.2. Step 2/3 - Register a BitDefender Account

BitDefender Registration
My Account
Please create a BitDefender account, sign in to your existing account or choose to create your account later.
With an account, you can always stay connected to BitDefender.
Sign in to an existing BitDefender account
E-mail:
Password:
Sign In
Forgot your password?
You do not have an account or you did not enter your log in information.
Create a new BitDefender account
Create an account later
< Back
Next >
Cancel

Account Registratiion

I do not have a BitDefender account

To create a BitDefender account, select **Create a new BitDefender account** and provide the required information. The data you provide here will remain confidential.

Note
If you want to create an account later, select the corresponding option.

- **E-mail** - type in your e-mail address.
- **Password** - type in a password for your BitDefender account. The password must be at least four characters long.
- **Re-type password** - type in again the previously specified password.
- **First name** - type in your first name.
- **Last name** - type in your last name.
- **Country** - select the country you reside in.

Note

Use the provided e-mail address and password to log in to your account at http://myaccount.bitdefender.com.

Click **Create account**.

To successfully create an account you must first activate your e-mail address. Check your e-mail address and follow the instructions in the e-mail sent to you by the BitDefender registration service.

Click **Next** to continue.

I already have a BitDefender account

BitDefender will automatically detect if you have previously registered a BitDefender account on your computer. In this case, all you have to do is to click **Next**.

If you already have an active account, but BitDefender does not detect it, select **Sign in to an existing BitDefender account**, provide the e-mail address and the password of your account and click **Sign In**.

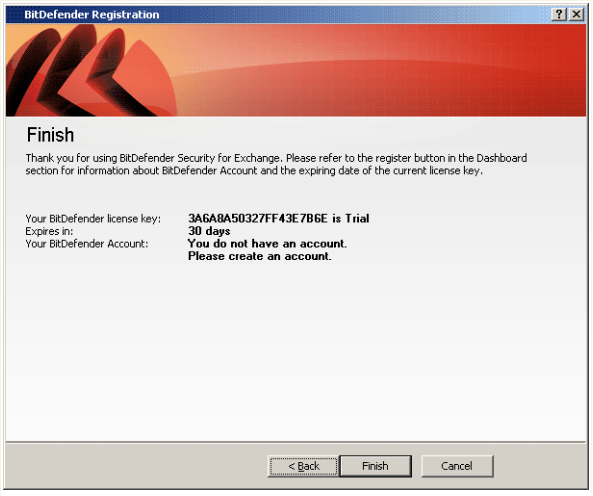
Note

If you provide an incorrect password, you will be prompted to re-type it when you click **Next**. Click **Ok** to enter the password again or **Cancel** to exit the wizard.

If you have forgotten your password, click **Forgot your password?** and follow the instructions.

Click **Next** to continue.

8.3. Step 3/3 - Finish


BitDefender Registration
Finish
Thank you for using BitDefender Security for Exchange. Please refer to the register button in the Dashboard section for information about BitDefender Account and the expiring date of the current license key.
Your BitDefender license key:
3A6A8A50327FF43E7B6E is Trial
Expires in:
30 days
Your BitDefender Account:
You do not have an account.
Please create an account.
< Back
Finish
Cancel

Finish

Click **Finish** to close the window.

Note
To log in to your BitDefender account, click **My account**.

9. Monitoring

The Monitoring snap-in provides you with all the necessary means to monitor and control the product activity.

If you click **Monitoring** in the tree menu, the dashboard will be displayed. The dashboard provides you with useful information on the status of BitDefender Security for Exchange and helps you easily solve the issues that require your attention.

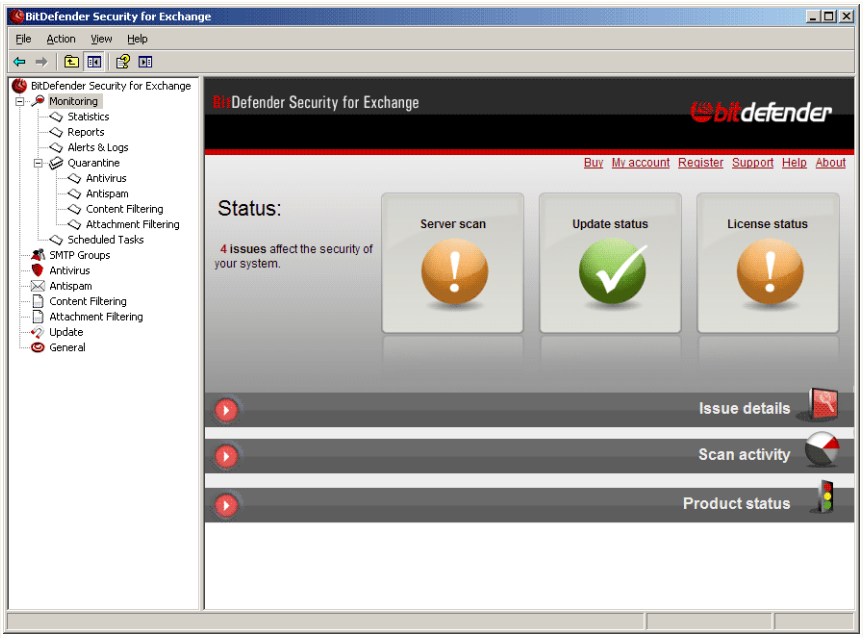
In the tree menu, grouped under the Monitoring snap-in, you can access the following sections:

- Statistics - provides real-time statistic information regarding the activity of the Antivirus, Antispam, Content and Attachment Filtering modules, both separately and as a whole.
- Reports - allows creating customized reports on the product activity.
- Alerts & Logs - allows configuring the logging options and sending alerts about the events that occur during product operation, such as an update error or an infected file detected.
- Quarantine - shows the quarantined files and mails. These objects were found to be infected, suspect or spam, or they matched a content or an attachment filtering rule and were moved to the quarantine folder, according to the specified action. They are grouped into four categories (Antivirus, Antispam, Content Filtering, Attachment Filtering), based on the BitDefender component that detected them.
- Scheduled Tasks - allows creating scheduled tasks through an intuitive wizard. You can schedule updates, on-demand scanning processes and reports to be generated.

In this chapter, you can find a detailed description of each section.

9.1. Dashboard

Click **Monitoring** in the tree menu to see the dashboard.



Dashboard

The dashboard provides you with useful information on the status of BitDefender Security for Exchange and helps you easily solve the issues that require your attention. You should check the dashboard frequently in order to quickly identify and solve the issues affecting the security of the Exchange server.

9.1.1. Important Links

At the top of the dashboard there are several useful links.

Link	Description
Buy	Opens a web page where you can buy the product from.
My Account	Opens your BitDefender account web page.
Register	Opens the registration wizard.
Support	Opens the BitDefender support web page.
Help	Opens the help file.
About	Opens a window where you can see details about the product.

9.1.2. Status Area

The **Status** area contains information about and helps you fix the existing issues.

Three status buttons, monitoring three categories of issues, immediately inform you about the existence of specific issues:

- Server scan
- Update status
- License status

Note
The License Status button and the related issues are not available if BitDefender Security for Exchange is managed by BitDefender Management Server.

To the left of the status buttons you can see the number of issues affecting the security of the Exchange server, if any.

The status buttons can be displayed in green, orange or red, depending on the existing issues that affect the security of the Exchange server:

- **Green** indicates that no issue requires your attention.
- **Orange** indicates the existence of issues that pose medium security risks. These issues do not require your immediate attention, but you should check them as soon as possible.
- **Red** indicates the existence of critical security issues, which require your immediate attention.

To find out details about these issues, do one of the following:

- Click a status button to see the respective category of issues.
- Click corresponding to **Issue details** to expand this section and see all possible issues.

The **Issue details** section contains three tables, one for each status button. Each table displays the monitored items and their current status. When there is an issue concerning one of the monitored items, a red **Fix** link is displayed. To quickly solve the existing issues, click the **Fix** links, one by one, or the **Fix all issues** button.

Important

For every monitored item, there is a check box selected by default in the **Monitor** column. If you do not want a specific item to be monitored, just clear the corresponding check box.

Server Scan

If the Server Scan button is orange or red, there are issues affecting the scanning activity of BitDefender Security for Exchange (its core modules).

Click the button to see the respective issues. A table named **Server scan** will be displayed and you will be able to see the monitored items and their current status.

- **Real-time protection.** The issues that can be reported are listed in the following table:

Status	*Description*
Scan files is off	Critical issue. Real-time protection is disabled and the Exchange server is not protected against malware. Click **Fix** to enable real-time protection.
Registration has expired	Critical issue. The licensing period has expired. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.

- **Antispam.** The issues that can be reported are listed in the following table:

Status	Description
Not enabled	Critical issue. Antispam filtering is disabled and the Exchange server is not protected against spam. Click **Fix** to enable antispam filtering.

- **Content Filtering.** The issues that can be reported are listed in the following table:

Status	Description
Not configured	Requires attention. Content filtering is enabled, but no content filtering rule is configured. Click **Fix** to go to Content Filtering > Policies and create appropriate rules.
Not enabled	There are two situations: 1. Requires attention. Content filtering is not enabled, but content filtering rules or policies are configured. Click **Fix** to enable content filtering. 2. Not an issue. Content filtering is not enabled and no content filtering rule is configured.

- **Attachment Filtering.** The issues that can be reported are listed in the following table:

Status	Description
Not configured	Requires attention. Attachment filtering is enabled, but no content filtering rule is configured. Click **Fix** to go to Attachment Filtering > Policies and create appropriate rules.
Not enabled	There are two situations: 1. Requires attention. Attachment filtering is not enabled, but attachment filtering rules or policies are configured. Click **Fix** to enable attachment filtering.

Status	Description
	2. Not an issue. Attachment filtering is not enabled and no attachment filtering rule is configured.

Update Status

If the Update Status button is orange or red, there are update issues affecting BitDefender Security for Exchange.

Click the button to see the respective issues. A table named **Update Status** will be displayed and you will be able to see the monitored items and their current status.

- **Last signature update.** The issues that can be reported are listed in the following table:

Status	Description
At least one update location failed	Critical issue. Contacting one or both update locations was not possible during the last update process. Click **Fix** to initiate a new update.
No update was performed	Critical issue. Click **Fix** to initiate a new update. The status will change to **Updating (%percent)**.
Update failed because the updates on your server are not signed, and you chose not to allow unsigned updates	Critical issue. You need to go to Update > Locations and select the **Allow unsigned updates** check box for your server.

- **Last product update.** The issues that can be reported are listed in the following table:

Status	Description
Product update disabled	Critical issue. Automatic product updates are disabled, making you server more vulnerable to security threats. Click **Fix** to enable automatic product updates.

Status	Description
Product update downloaded, please install it	Critical issue. A new product update has been downloaded and it is not installed on your system. Clicking **Fix** will install the update. If the update requires stopping traffic or rebooting the server, you will have to confirm your choice by clicking **OK**. To be able to schedule the installation of available product updates that require stopping traffic or rebooting the server, click the **Fix all issues** button instead.
A new kit is available and it is not installed on your system	Critical issue. The new kit may come with new features and functionalities. Click **Fix** to install the kit. You will have to confirm your choice by clicking **OK**. Please note that installing the kit might require a server restart.

- **Signature update older than one day.** The issues that can be reported are listed in the following table:

Status	Description
Updates are old	Critical issue. More than one day passed since the last update. Click **Fix** to initiate a new update. The status will change to **Updating (%percent)**.

- **Automatic update.** The issues that can be reported are listed in the following table:

Status	Description
Automatic update is off and no scheduled update task is defined and on	Critical issue. BitDefender Security for Exchange is not automatically updated on a regular basis. Click **Fix** to enable automatic update. If not already configured, the update interval is set to one hour.

License Status

If the License Status button is orange or red, there are issues concerning the license of your BitDefender Security for Exchange.

Note
The License Status button and the related issues are not available if BitDefender Security for Exchange is managed by BitDefender Management Server.

Click the button to see the respective issues. A table named **License Status** will be displayed and you will be able to see the monitored items and their current status.

- **Registration.** The issues that can be reported are listed in the following table:

Status	*Description*
You are using a trial version of the product and you should register it	Requires attention. This status is displayed during the trial period. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.
Your product registration will expire in x days. You should renew your registration	Requires attention. This status is displayed during the last 30 days of the licensing period. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.
Product registration expired. You should register it	Critical issue. The licensing period has expired. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.
The serial number you introduced is not valid	Requires attention. You have entered an invalid license key. Click **Fix** to open the registration wizard where you can register BitDefender Security for Exchange with a new license key.

- **My account.** The issues that can be reported are listed in the following table:

Status	Description
You do not have an account. Please create an account	Requires attention. You have not registered an account yet. Click **Fix** to open the registration wizard and create a new account or provide the details of an existing one.
The password you introduced is incorrect. Please try again	Click **Fix** to open the registration wizard where you can create a new account or log in to an existing one.
Server error! Please try again later	Requires attention. A connection with the BitDefender server could not be established. Click **Fix** to open the registration wizard and try again.
Account locked	Click **Fix** to open the registration wizard where you can create a new account or log in to an existing one.

- **Registration will expire alert.** The issues that can be reported are listed in the following table:

Status	Description
You have x days remaining from your license key	Requires attention. This status is displayed during the last 30 days of the licensing period. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.
Product is expired	Critical issue. The licensing period has expired. Click **Fix** to open the registration wizard and register BitDefender Security for Exchange with a new license key.

9.1.3. Scan Activity

To see graphical statistics regarding the scanning activity of BitDefender Security for Exchange, click corresponding to the **Scan activity** section.

The statistics are grouped based on the core modules: Antivirus, Antispam, Content Filtering and Attachment Filtering.

9.1.4. Product Status

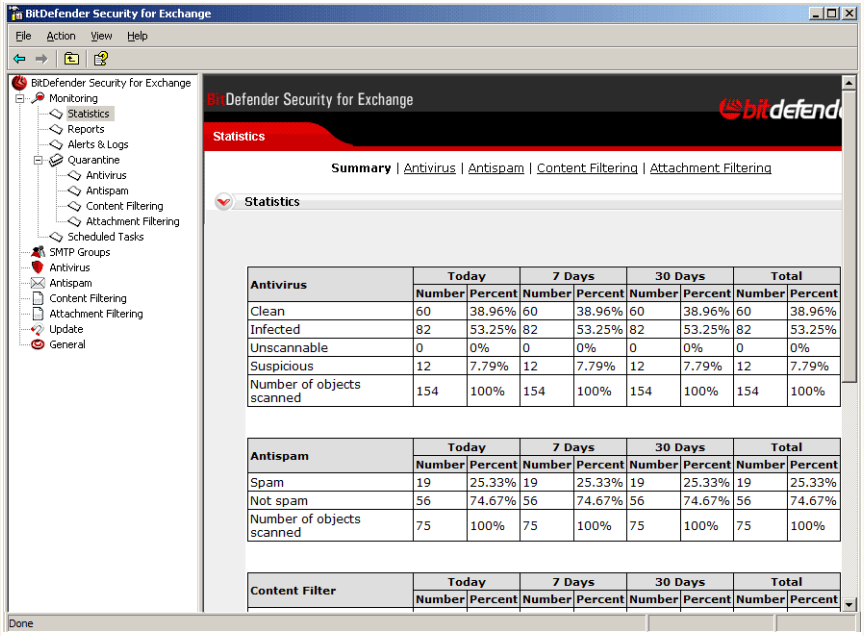
To see information on the product status, click corresponding to the **Product status** section.

You can see the name of the server BitDefender Security for Exchange is installed on, as well as the product version and the number of available malware signatures.

9.2. Statistics

There is a special BitDefender database which stores information regarding the product's activity. Based on this database, BitDefender offers the possibility to obtain real-time statistical data regarding the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules, both separately and as a whole.

If you want to see detailed statistics regarding the real-time scanning activity of BitDefender Security for Exchange, click **Statistics** in the tree menu under **Monitoring**.


BitDefender Security for Exchange
File Action View Help
BitDefender Security for Exchange
Monitoring
Statistics
Reports
Alerts & Logs
Quarantine
Antivirus
Antispam
Content Filtering
Attachment Filtering
Scheduled Tasks
SMTP Groups
Antivirus
Antispam
Content Filtering
Attachment Filtering
Update
General
BitDefender Security for Exchange
Statistics
Summary | Antivirus | Antispam | Content Filtering | Attachment Filtering
Statistics
Antivirus | Today | 7 Days | 30 Days | Total
Number | Percent | Number | Percent | Number | Percent | Number | Percent
Clean | 60 | 38.96% | 60 | 38.96% | 60 | 38.96% | 60 | 38.96%
Infected | 82 | 53.25% | 82 | 53.25% | 82 | 53.25% | 82 | 53.25%
Unscannable | 0 | 0% | 0 | 0% | 0 | 0% | 0 | 0%
Suspicious | 12 | 7.79% | 12 | 7.79% | 12 | 7.79% | 12 | 7.79%
Number of objects scanned | 154 | 100% | 154 | 100% | 154 | 100% | 154 | 100%
Antispam | Today | 7 Days | 30 Days | Total
Number | Percent | Number | Percent | Number | Percent | Number | Percent
Spam | 19 | 25.33% | 19 | 25.33% | 19 | 25.33% | 19 | 25.33%
Not spam | 56 | 74.67% | 56 | 74.67% | 56 | 74.67% | 56 | 74.67%
Number of objects scanned | 75 | 100% | 75 | 100% | 75 | 100% | 75 | 100%
Content Filter | Today | 7 Days | 30 Days | Total
Number | Percent | Number | Percent | Number | Percent | Number | Percent
Done

Statistics

There are five main windows which provide real-time statistical information on the overall product activity and the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules. Each of these categories contains several types of statistics grouped into 4 time intervals: current day, last week, last month and total. Click a link to access the corresponding statistics.

The following types of statistics are available:

- **Summary.** Provides overall statistics on the activity of BitDefender Security for Exchange.
- **Antivirus.** Contains the statistics on the Antivirus module.

Type	*Description*
Antivirus Summary	Provides overall statistics on the activity of the Antivirus module.

Type	Description
Top Malware	Shows the top of the malware detected.
Top Malware Senders	Lists mail senders based on the quantity of malware sent.
Top Malware Recipients	Lists mail recipients based on the quantity of malware received.

- **Antispam.** Contains the statistics on the Antispam module.

Type	Description
Antispam Summary	Provides overall statistics on the activity of the Antispam module.
Top Spam Senders	Lists mail senders based on the spam volume sent.

- **Content Filtering.** Contains the statistics on the Content Filtering module.

Type	Description
Content Filtering Summary	Provides overall statistics on the activity of the Content Filtering module.
Top Volume Senders	Lists mail senders based on the number of content filtering rules matched.
Top Volume Recipients	Lists mail recipients based on the number of content filtering rules matched.

- **Attachment Filtering.** Contains the statistics on the Attachment Filtering module.

Type	Description
Attachment Filtering Summary	Provides overall statistics on the activity of the Attachment Filtering module.
Top Attachment Volume Senders	Lists mail senders based on the number of attachment filtering rules matched.
Top Attachment Volume Recipients	Lists mail recipients based on the number of attachment filtering rules matched.

9.2.1. Clearing All Records

By default, BitDefender automatically erases statistical information older than one week. If you wish to keep the statistical information for a different period of time, click the **Purge Options** button and set the number of days / weeks / months for which statistics are to be stored.

Note
Statistics older than the specified period will be automatically deleted.

In case you wish to clear the database of information regarding product activity you need to follow these steps:

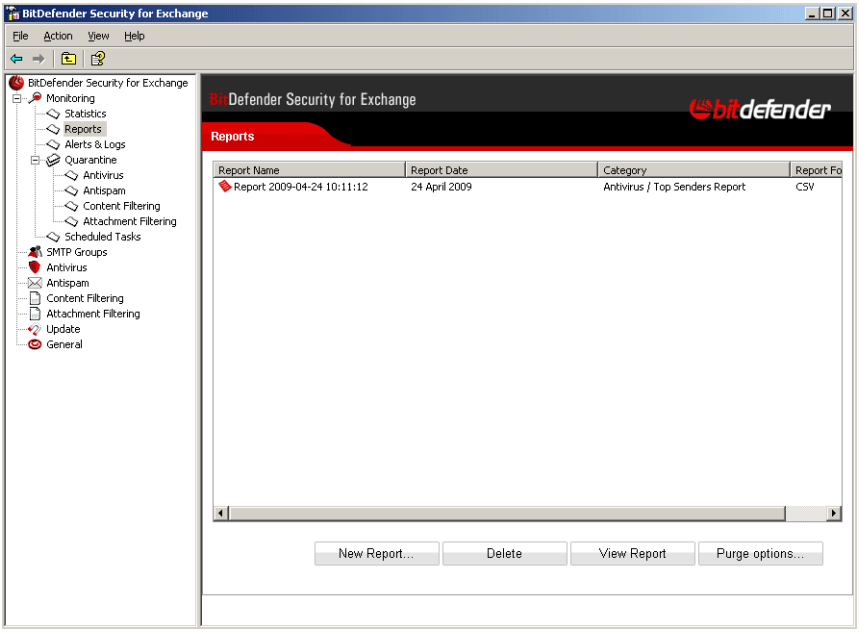
1. Right-click **Statistics** in the tree menu, a contextual menu will appear.
2. Select **Clear all records**.
3. Click **Yes** to confirm your choice.

Note
The Statistics module shares its database with the Reports module. Creating new reports for the period prior to the data clearing will no longer be possible.

9.3. Reports

The same BitDefender database used by the Statistics module can also be used to create customized reports regarding the activity of the Antivirus, Antispam, Content Filtering and Attachment Filtering modules. Reports contain general information (the report name, the time interval for which the report is generated and the server name) and specific information which depends on the type of report. They can be generated in HTML, text or comma-separated values (CSV) format.

To create, view and manage reports, go to **Reports** in the tree menu under **Monitoring**.



Reports

You can see all the existing reports listed in the table. For each report, the following information is provided: the report name, the date when the report was generated, the type of information it contains and the format.

You can create the following types of reports:

- **Antivirus.** Create custom reports with information on the activity of the Antivirus module.

Report Type	*Description*
Total	Provides complete information on the activity of the Antivirus module.
Top Malware	Provides a table containing the malware detected, in descending order.

Report Type	Description
Top Malware Senders	Contains the mail senders ordered by the quantity of malware sent.
Top Malware Recipients	Contains the mail recipients ordered by the number of malware received.

- **Antispam.** Create custom reports with information on the activity of the Antispam module.

Report Type	Description
Total	Provides complete information on the activity of the Antispam module.
Top Spam Senders	Contains the mail senders ordered by the spam volume sent.
Total by filters	Contains a top of malware ordered by the antispam filters that caught them.

- **Content Filtering.** Create custom reports with information on the activity of the Content Filtering module.

Report Type	Description
Total	Provides complete information on the activity of the Content Filtering module.
Top Volume Senders	Contains the mail senders ordered by the number of content filtering rules matched.
Top Volume Recipients	Contains the mail recipients ordered by the number of content filtering rules matched.

- **Attachment Filtering.** Create custom reports with information on the activity of the Attachment Filtering module.

Report Type	Description
Total	Provides complete information on the activity of the Attachment Filtering module.
Top Volume Senders	Contains the mail senders ordered by the number of attachment filtering rules matched.
Top Volume Recipients	Contains the mail recipients ordered by the number of attachment filtering rules matched.

9.3.1. Managing Reports

To manage the reports, use the provided buttons:

- **New Report** - launches a wizard that will help you create a new report.
- **Delete** - deletes one or several selected report files. You will have to confirm your choice by clicking **Yes**.
- **View Report** - opens a selected report file.

Note
To view a report you can also double-click it.

- **Purge Options** - opens a new window where you can specify how long report files should be kept. Enter the number of hours / days / weeks / months during which to store reports and click **OK** to save changes.

Note
Reports older than the specified period will be automatically deleted.

9.3.2. Creating Reports

To create reports on the product activity, click **New Report** and follow the wizard that will appear.

Note
To launch the Report Wizard you can also right click **Reports** in the tree menu and select **New Report...** in the contextual menu.

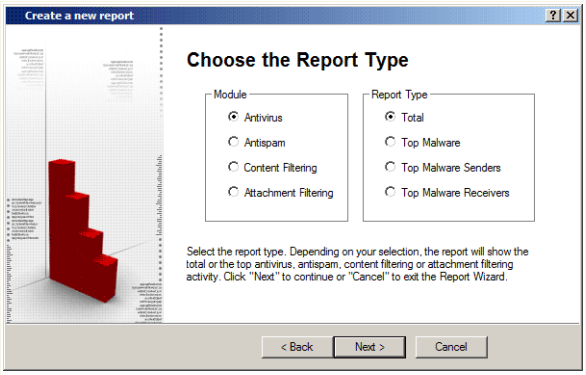
Step 1/5 - Welcome to the Report Wizard

Create a new report
Welcome to BitDefender Security for Exchange Report Wizard!
Report Wizard guides you through the steps required to generate a report regarding the activity of the BitDefender Security for Exchange product installed on the server. Click "Next" to continue or click "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Welcome

Click **Next** to continue or **Cancel** to quit.

Step 2/5 - Select Report Type


Create a new report
Choose the Report Type
Module
Antivirus
Antispam
Content Filtering
Attachment Filtering
Report Type
Total
Top Malware
Top Malware Senders
Top Malware Receivers
Select the report type. Depending on your selection, the report will show the total or the top antivirus, antispam, content filtering or attachment filtering activity. Click "Next" to continue or "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Report Type

First, you must select the module the generated report is on: **Antivirus**, **Antispam**, **Content Filtering** or **Attachment Filtering**.

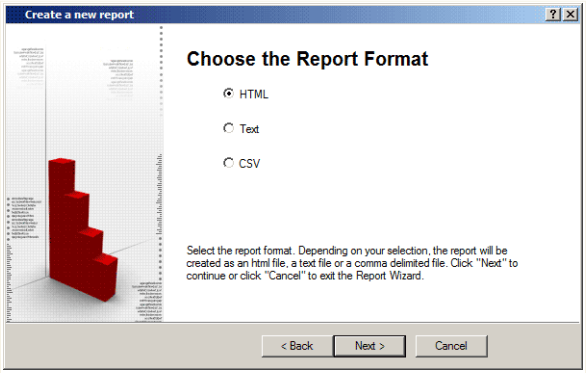
Then select one of the report types available for the module you have chosen.

Note
For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 52) section.

Depending on your choice, the report may contain a summary of or only specific data about the activity of a specified component.

Click **Next**.

Step 3/5 - Select Report Format

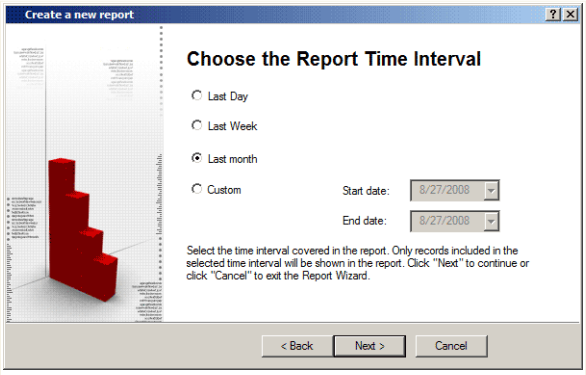

Create a new report
Choose the Report Format
HTML
Text
CSV
Select the report format. Depending on your selection, the report will be created as an html file, a text file or a comma delimited file. Click "Next" to continue or click "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Report Format

Select the format of the report file (**HTML**, **text** or **CSV**). Depending on your selection, the report will be created as an HTML, text or comma-separated values (CSV) file.

Click **Next**.

Step 4/5 - Select Time Interval


Create a new report
Choose the Report Time Interval
Last Day
Last Week
Last month
Custom
Start date:
8/27/2008
End date:
8/27/2008
Select the time interval covered in the report. Only records included in the selected time interval will be shown in the report. Click "Next" to continue or click "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Time Interval

Select the time interval covered in the report:

- **Last day**
- **Last week**
- **Last month**
- **Custom**

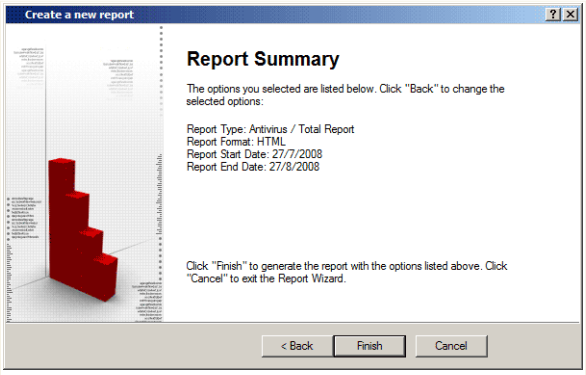
If you need information about the BitDefender activity related to a specific time interval, select **Custom** and specify the start and end date. To specify the start and end date, either click the numbers in the date field and enter new values or click **the arrow** to choose a date from the calendar.

Note
The date format is month/day/year.

Only the records from the specified period will appear in the report.

Click **Next**.

Step 5/5 - View Summary


Create a new report
Report Summary
The options you selected are listed below. Click "Back" to change the selected options:
Report Type: Antivirus / Total Report
Report Format: HTML
Report Start Date: 27/7/2008
Report End Date: 27/8/2008
Click "Finish" to generate the report with the options listed above. Click "Cancel" to exit the Report Wizard.
< Back
Finish
Cancel

View Summary

This window displays the selected report settings. You can make any changes by returning to the previous steps (click **Back**).

Click **Finish** to generate the report. The report will appear in the Reports section.

9.4. Alerts & Logs

The Alerts & Logs snap-in allows configuring the BitDefender notification system.

BitDefender is by default configured to keep a log of its activity. The BitDefender log provides you with a comprehensive list of the events that occured during product operation. To configure logging or view the log files, go to the Logs tab.

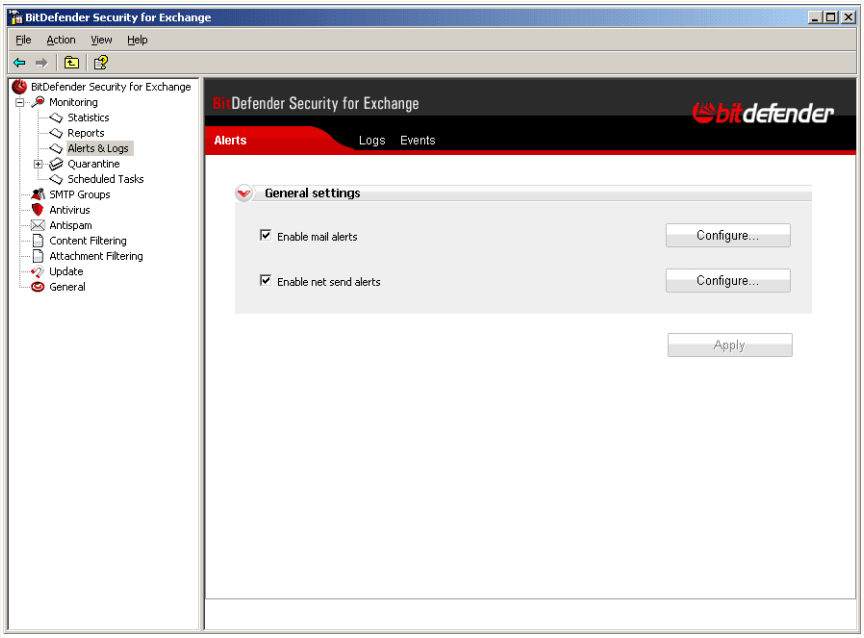
Moreover, you can configure BitDefender to immediately alert designated people about the occurrence of certain events during product operation. Alerts can be sent through mail or using the `net send` command. To configure the mail and net send alert notification services, go to the Alerts tab.

You can completely disable notifications for each event or you can configure BitDefender to send mail and net send alerts when the event occurs. To specify the notification methods for each event, go to the Events tab. For more information, please refer to "*Configuring Events*" (p. 70).

9.4.1. Alerts

Alerts are messages that include product-related information and which are meant to inform their recipients about the product activity. BitDefender can be set to notify users and administrators about occurring events through mail or net send alerts.

To configure the alert notification services, click **Alerts & Logs** in the tree menu (under **Monitoring**) and then the **Alerts** tab.



Alerts

Mail Alerts

BitDefender can notify the network administrator by sending configurable mail alerts in case an event for which they have been set takes place. Enabling this alert will provide you with relevant and timely information about the status of your server, and may eliminate the need to access the BitDefender management console.

Note
This module integrates with an SMTP Server. It works with an ESMTP server as well, but it does not use the ESMTP protocol because it is implemented on SMTP.

In order to use the mail notification service, follow these steps:

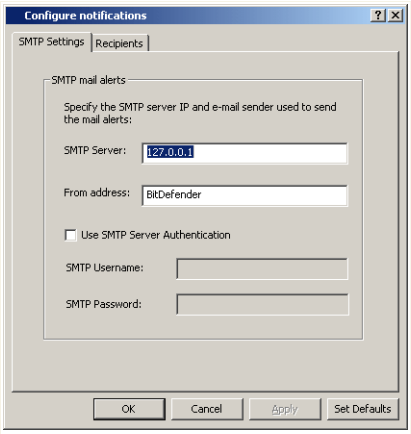
1. Select **Enable Mail Alerts** to activate the mail notification service and then click **Apply** to save the changes.

2. Configure the SMTP settings, as described in the "*Configuring Mail Alert Settings*" (p. 62) section.
3. Configure the recipients of the mail alerts, as described in the "*Configuring Mail Alert Recipients*" (p. 63) section.
4. Go to the Events tab and configure the events for which mail alerts should be sent, as described in the "*Configuring Events*" (p. 70) section.

If you want to disable this service, clear the check box corresponding to **Enable Mail Alerts** and then click **Apply** to save the changes.

Configuring Mail Alert Settings

To configure the SMTP settings of mail alerts click the corresponding **Configure** button. A new window will appear.



SMTP Settings

Specify the SMTP settings required for sending the mail alerts.

- **SMTP Server** - type in the IP address of the SMTP server that your network uses to send messages.
- **From address** - type in the e-mail address that will appear in the sender field.

Important
Provide a valid e-mail address for the SMTP server, otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

- If the SMTP server used to send messages requires authentication, select **Use SMTP Server Authentication** and enter the user name and password in the corresponding fields.

Note
NTLM authentication is not supported.

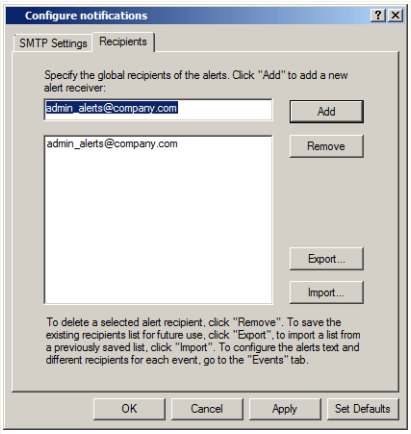
Click **Apply** to save the changes and **OK** to close the window.

Configuring Mail Alert Recipients

To configure the recipients of the mail alerts click the corresponding **Configure** button and then the **Recipients** tab. A new window will appear.

Note

The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set. To specify different recipients for each event, go to the Events tab and configure the events. For more information, please refer to "*Configuring Events*" (p. 70).


Configure notifications
SMTP Settings
Recipients
Specify the global recipients of the alerts. Click "Add" to add a new alert receiver:
admin_alerts@company.com
Add
admin_alerts@company.com
Remove
Export...
Import...
To delete a selected alert recipient, click "Remove". To save the existing recipients list for future use, click "Export", to import a list from a previously saved list, click "Import". To configure the alerts text and different recipients for each event, go to the "Events" tab.
OK
Cancel
Apply
Set Defaults

Recipients

Provide the e-mail address in the corresponding field and click **Add** to add the recipient to the list.

To import e-mail addresses from a `txt` file, click **Import**, select the file and then click **Open**.

If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected recipients click **Remove**.

Click **Apply** to save the changes and **OK** to close the window.

Net Send Alerts

BitDefender can notify the network administrator by sending configurable alerts through the `net send` command upon the occurrence of an event for which they have been set.

Note

This module integrates with the Net Send command of the Windows Operating System on which the product is installed and it provides alerts regarding the product activity. In order to receive such alerts, the Messenger and Alert services must be enabled by the administrator on the server and on the client workstations.

In order to use the net send notification service, follow these steps:

1. Select **Enable Net Send Alerts** to activate the net send notification service and then click **Apply** to save the changes.
2. Configure the recipients of the net send alerts, as described in the "*Configuring Net Send Alert Recipients*" (p. 65) section.
3. Go to the Events tab and configure the events for which net send alerts should be sent, as described in the "*Configuring Events*" (p. 70) section.

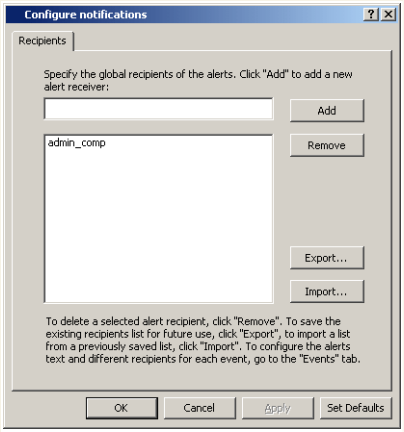
If you want to disable this service, clear the check box corresponding to **Enable Net Send Alerts** and then click **Apply** to save the changes.

Important
In case of a virus outbreak it is not advisable to use this type of alert.

Configuring Net Send Alert Recipients

To configure the recipients of the net send alerts click the corresponding **Configure** button. A new window will appear.

Note
The recipients specified here will be alerted upon the occurrence of an event for which this type of alert has been set. To specify different recipients for each event, go to the Events tab and configure the events. For more information, please refer to "*Configuring Events*" (p. 70).


Configure notifications
Recipients
Specify the global recipients of the alerts. Click "Add" to add a new alert receiver:
Add
admin_comp
Remove
Export...
Import...
To delete a selected alert recipient, click "Remove". To save the existing recipients list for future use, click "Export", to import a list from a previously saved list, click "Import". To configure the alerts text and different recipients for each event, go to the "Events" tab.
OK
Cancel
Apply
Set Defaults

Recipients

Provide the computer name in the corresponding field and click **Add** to add the recipient to the list.

To import computer names from a `txt` file, click **Import**, select the file and then click **Open**.

If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected recipients click **Remove**.

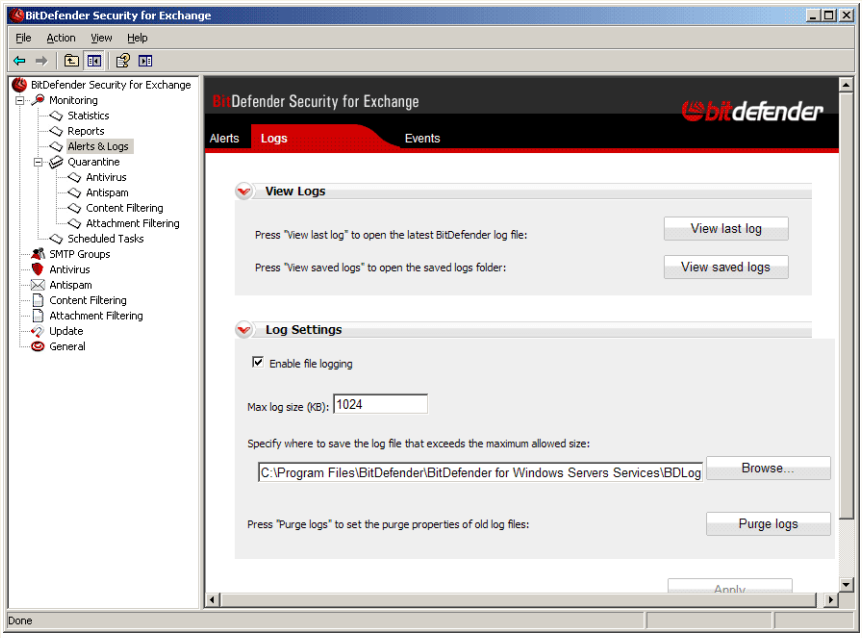
Click **Apply** to save the changes and **OK** to close the window.

9.4.2. Logs

BitDefender is by default configured to keep a log of its activity. The BitDefender log provides you with a comprehensive list of the events that occured during product operation.

Note
By default, the log file is saved in: ?:\Program Files\BitDefender\BitDefender for Windows Servers Services\BDLog.

To configure logging and to view the log files, click **Alerts & Logs** in the tree menu (under **Monitoring**) and then the **Logs** tab.



Logs

Configuring Logging

To log the product activity to a file, select **Enable file logging**.

BitDefender creates the log file in `?:\Program Files\BitDefender\BitDefender for Windows Servers Services\BDLog`. By default, when the file reaches the size limit of 1024 KB, a new log file is created.

Specify the size limit of the log files in the **Maximum log file size** field. If you do not want to limit the size of the log file, enter 0 in the edit field.

You can specify a folder where files exceeding the specified size limit should be saved. Either provide its path in the corresponding field or click **Browse**, locate the folder and then click **OK** to set the location.

To set the time period for which logs are to be stored, click **Purge logs**. Enter the number of hours / days / weeks / months during which to store reports and click **OK**.

Click **Apply** to save the changes.

Examining Logs

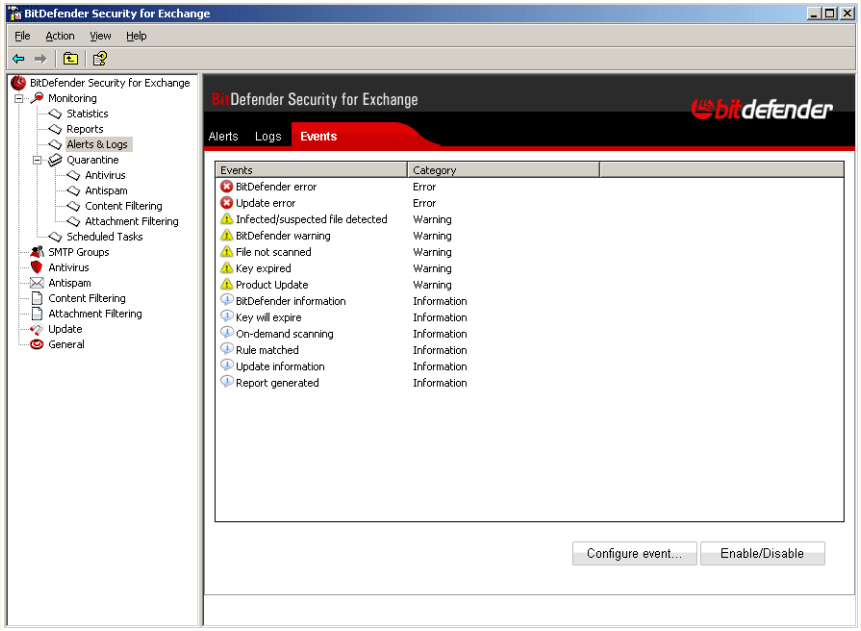
Click **View last log** to open the last log file.

If you have set a size limit for the log file, you can see any saved log file. Click **View saved logs**, locate the log file you want to see and double-click it.

9.4.3. Events

You can completely disable notifications for each event or you can configure BitDefender to send mail and net send alerts when the event occurs.

To specify the notification methods for each event, click **Alerts & Logs** in the tree menu (under **Monitoring**) and then the **Events** tab.



Events

All of the events that may occur are listed in the table. There are 3 types of events:

- **Information** - such events provide information about the product activity.
- **Warning** - such events provide critical information about aspects of the product activity which require your attention.
- **Error** - such events provide information about errors that appear during product operation.

Here is the list of the events that may appear:

Event	*Description*
BitDefender Error	Groups all the errors that may appear during product operation, such as service start failure.

Event	Description
Update Error	Refers to the occurrence of an error during the update process.
Infected/suspected file detected	Occurs when an infected file or a file suspected of being infected has been detected.
BitDefender Warning	Groups critical information regarding the activity of BitDefender.
File not scanned	Occurs when a file could not be scanned by BitDefender.
Key expired	Indicates the expiration of the registration period.
Product update	Occurs when a product update is available.
BitDefender information	Groups information regarding the activity of BitDefender.
Key will expire	Indicates that there are 3 days left before the product expires.
On-demand scanning	Occurs whenever an on-demand scan is performed.
Rule matched	Occurs whenever a message matches a Content Filtering or Attachment Filtering rule.
Update information	Contains information about the update process.
Report generated	Occurs whenever a report is generated.

Managing Events

To manage the events, use the provided buttons:

- **Configure event** - opens the configuration window of a selected event, allowing you to configure the importance level of the event and, if necessary, the mail and net send alerts issued when the event occurs. For more information, please refer to "*Configuring Events*" (p. 70).
- **Enable / Disable** - enables / disables event notification for one or several selected events.

Note
If event notification is disabled, the event is not logged and no alert is sent when it takes place.

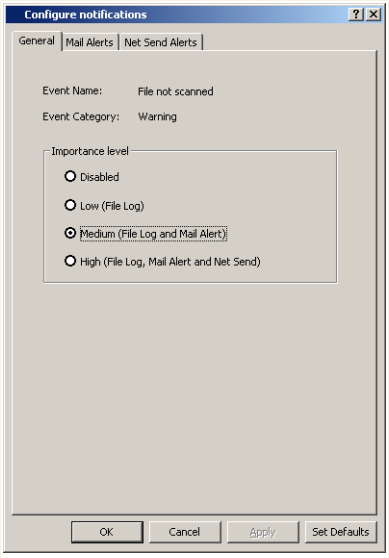
Configuring Events

You can configure the notification methods separately for each event in the list. To configure the notification methods for a specific event, select it and click **Configure event**. The configuration window will appear.

Follow these steps to configure event notification:

Step 1/3 - Select Event Importance

Open the configuration window to select the importance of the event.



Select Event Importance

You can see the name and category of the event.

When an event takes place, based on its importance, it can be logged and, possibly, specified recipients may be notified through mail and net send alerts of its occurrence. Choose one of the following options to set the importance level:

- **Disabled** - to disable event notification.

Note
If event notification is disabled, the event is not logged and no alert is sent when it takes place.

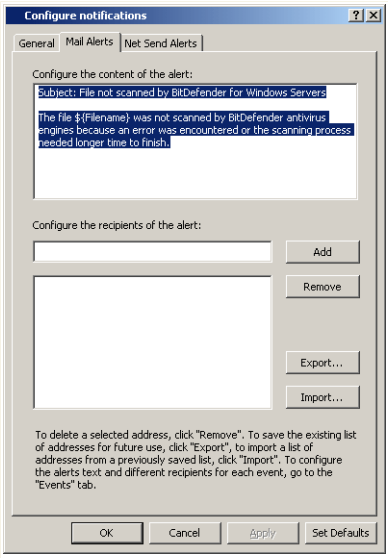
- **Low (File Log)** - to keep a record of the event in the log file. No alert is sent when the event takes place.
- **Medium (File Log and SMTP)** - to log the event and send mail alerts when the event takes place.
- **High (File Log, SMTP and Net Send)** - to log the event and send mail and net send alerts when the event takes place.

Note
To make sure that logging and the mail and net send notification services are enabled, go to the Logs and Alerts sections.

Click **Apply** to save the changes and **OK** if you want to close the window.

Step 2/3 - Configure Mail Alerts

If the importance of the event is medium or high, mail alerts will be sent. Click the **Mail Alerts** tab to configure the mail alerts.


Configure notifications
General
Mail Alerts
Net Send Alerts
Configure the content of the alert:
Subject: File not scanned by BitDefender for Windows Servers
The file $(Filename) was not scanned by BitDefender antivirus engines because an error was encountered or the scanning process needed longer time to finish.
Configure the recipients of the alert:
Add
Remove
Export...
Import...
To delete a selected address, click "Remove". To save the existing list of addresses for future use, click "Export", to import a list of addresses from a previously saved list, click "Import". To configure the alerts text and different recipients for each event, go to the "Events" tab.
OK
Cancel
Apply
Set Defaults

Configure Mail Alerts

Configure Alert Text

BitDefender allows you to configure the alert content. You can see the default text in the box.

Make the desired changes to the alert content.

Important
You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

Configure Alert Recipients

Provide the e-mail address in the corresponding field and click **Add** to add the recipient to the list.

Note
Beside the recipients defined here, the alert will also be sent to those defined in the Alerts section (see "*Configuring Mail Alert Recipients*" (p. 63)).

To import e-mail addresses from a `txt` file, click **Import**, select the file and then click **Open**.

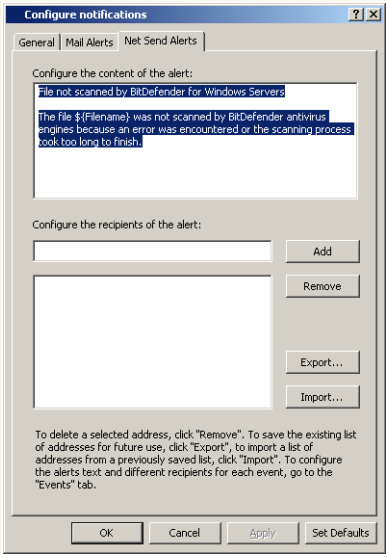
If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

To remove one or several selected recipients click **Remove**.

Click **Apply** to save the changes and **OK** if you want to close the window.

Step 3/3 - Configure Net Send Alerts

If the importance of the event is high, net send alerts will be sent. Click the **Net Send Alerts** tab to configure the net send alerts.


Configure notifications
General
Mail Alerts
Net Send Alerts
Configure the content of the alert:
File not scanned by BitDefender for Windows Servers
The file ${Filename} was not scanned by BitDefender antivirus engines because an error was encountered or the scanning process took too long to finish.
Configure the recipients of the alert:
Add
Remove
Export...
Import...
To delete a selected address, click "Remove". To save the existing list of addresses for future use, click "Export", to import a list of addresses from a previously saved list, click "Import". To configure the alerts text and different recipients for each event, go to the "Events" tab.
OK
Cancel
Apply
Set Defaults

Configure Net Send Alerts

Configure Alert Text

BitDefender allows you to configure the alert content. You can see the default text in the box.

Make the desired changes to the alert content.

Important
You should NOT modify the strings that begin with the $ symbol as they provide valuable information about the event.

Configure Alert Recipients

Provide the computer name in the corresponding field and click **Add** to add the recipient to the list.

Note
Beside the recipients defined here, the alert will also be sent to those defined in the Alerts section (see "*Configuring Net Send Alert Recipients*" (p. 65)).

To import computer names from a `txt` file, click **Import**, select the file and then click **Open**.

If you want to export the list to a `txt` file, click **Export** and save the file to the desired location.

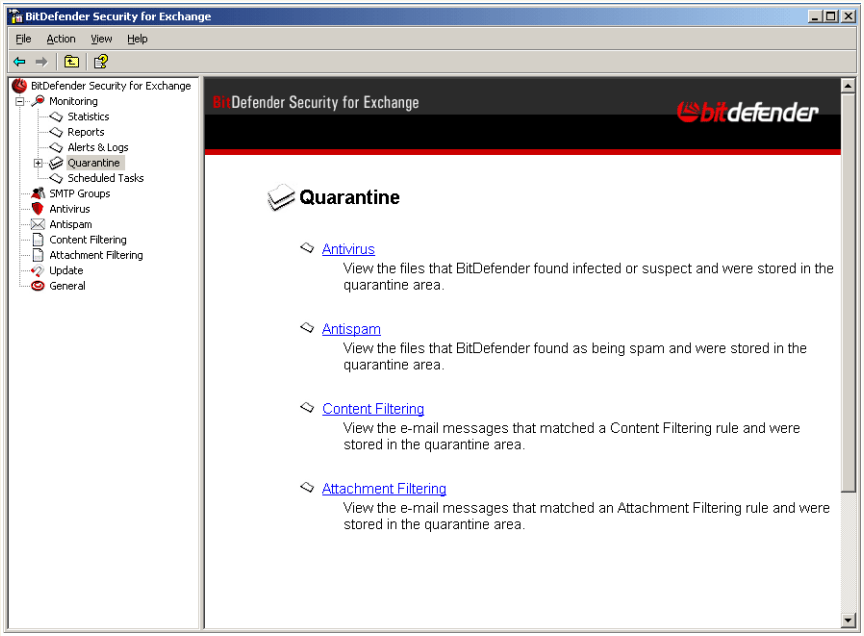
To remove one or several selected recipients click **Remove**.

Click **Apply** to save the changes and **OK** to close the window.

9.5. Quarantine

BitDefender allows isolating files in a secure area, named quarantine.

To see the quarantined files and manage them, click **Quarantine** in the tree menu (under **Monitoring**).


BitDefender Security for Exchange
File Action View Help
BitDefender Security for Exchange
Monitoring
Statistics
Reports
Alerts & Logs
Quarantine
Scheduled Tasks
SMTP Groups
Antivirus
Antispam
Content Filtering
Attachment Filtering
Update
General
BitDefender Security for Exchange
bitdefender
Quarantine
Antivirus
View the files that BitDefender found infected or suspect and were stored in the quarantine area.
Antispam
View the files that BitDefender found as being spam and were stored in the quarantine area.
Content Filtering
View the e-mail messages that matched a Content Filtering rule and were stored in the quarantine area.
Attachment Filtering
View the e-mail messages that matched an Attachment Filtering rule and were stored in the quarantine area.

Quarantine

Quarantine is divided into 4 areas:

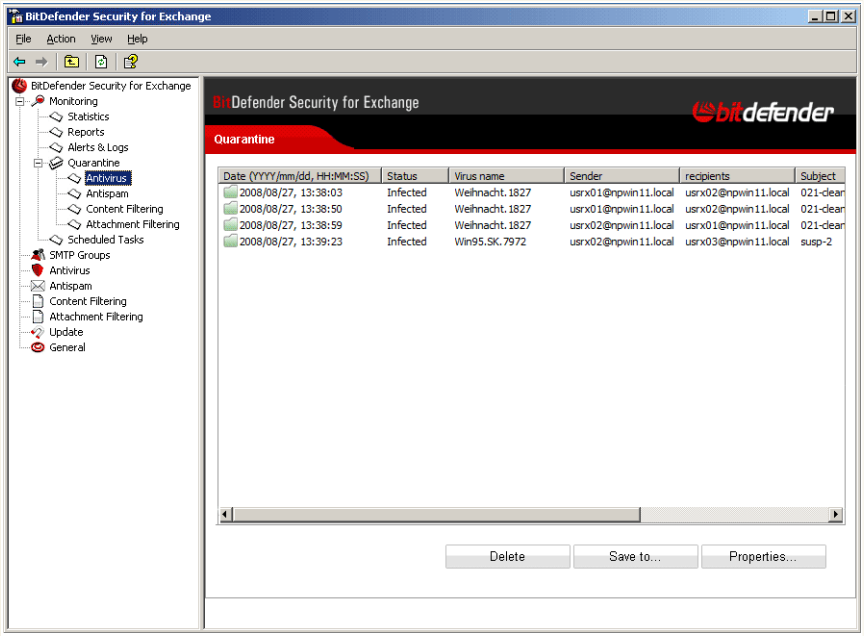
- Antivirus - contains the objects that BitDefender found infected or suspect and which were stored in the quarantine area.
- Antispam - contains the messages that BitDefender found as being spam and which were stored in the quarantine area.
- Content Filtering - contains the messages that matched a Content Filtering rule and which were stored in the quarantine area.

- Attachment Filtering - contains the messages that matched an Attachment Filtering and which were stored in the quarantine area.

Click a link to see the quarantined files for the corresponding component.

9.5.1. Antivirus Quarantine

Click **Antivirus** in the tree menu (**Quarantine** module) to enter this section.



Antivirus Quarantine

This is where you can see the objects that BitDefender found infected or suspect and which were stored in the quarantine area.

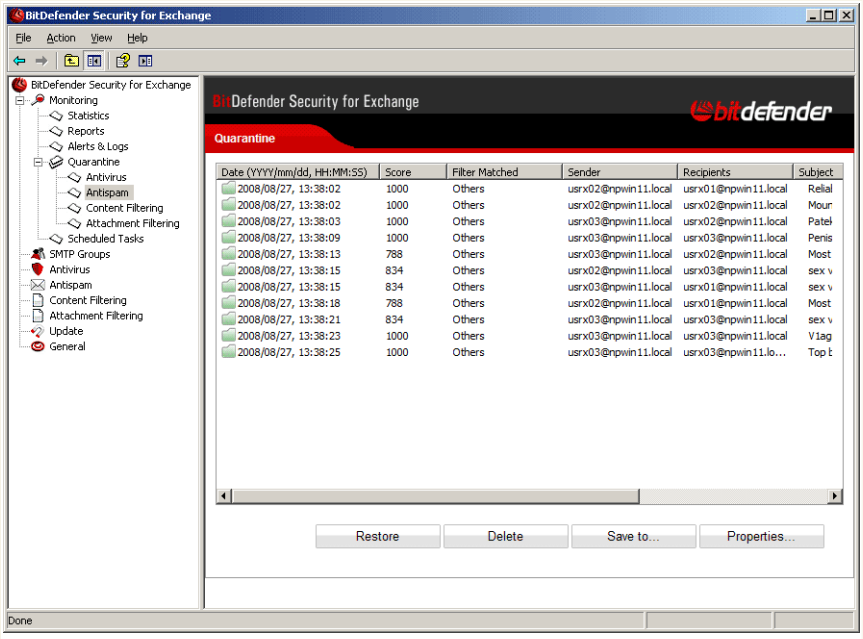
There are two types of quarantined objects: mail body and mail attachment. For each quarantined file, the following information is provided: the date and time when it was quarantined, the status (infected / suspect / unscanable), the virus name, the mail address or mailbox of the sender, the mail address or mailbox of the recipients, the subject of the message and the file name (for attachments).

Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. In this way you can analyze the item and send it by mail.

Note
To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 81).

9.5.2. Antispam Quarantine

Click **Antispam** in the tree menu (**Quarantine** module) to enter this section.



Antispam Quarantine

This is where you can see the messages that BitDefender found as being spam and which were stored in the quarantine area.

For each quarantined message, the following information is provided: the date and time when it was quarantined, the spam score received, the filter that classified it as

being spam, the mail address of the sender, the mail address of the recipients, the subject and the file name of the message.

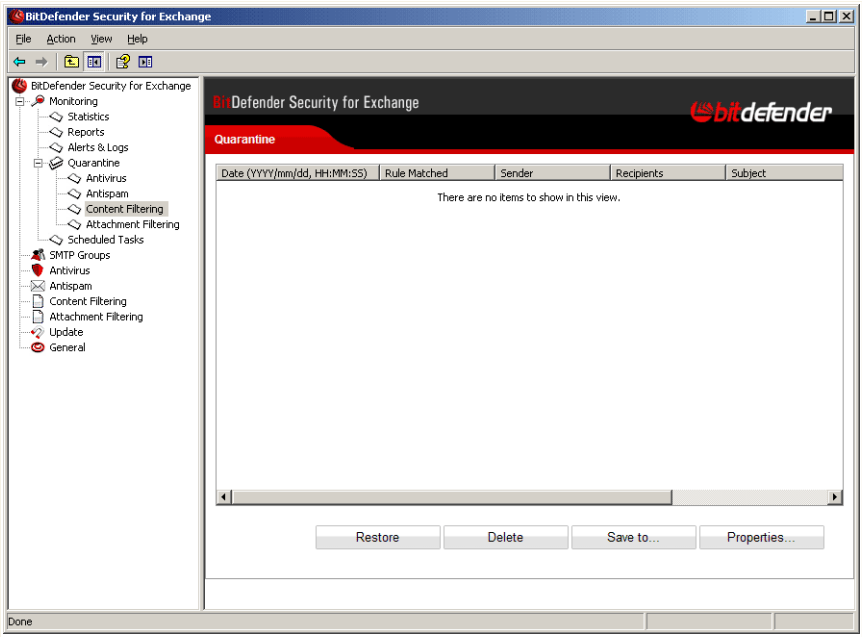
Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. In this way you can analyze the item and send it by mail.

To decrypt and deliver a quarantined message to its intended recipient, select the message and click **Restore**.

Note
To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 81).

9.5.3. Content Filtering Quarantine

Click **Content Filtering** in the tree menu (**Quarantine** module) to enter this section.



Content Filtering Quarantine

This is where you can see the messages that matched a Content Filtering rule and which were stored in the quarantine area.

For each quarantined message, the following information is provided: the date and time when it was quarantined, the matching rule, the mail address of the sender, the mail address of the recipients, the subject and the file name of the message.

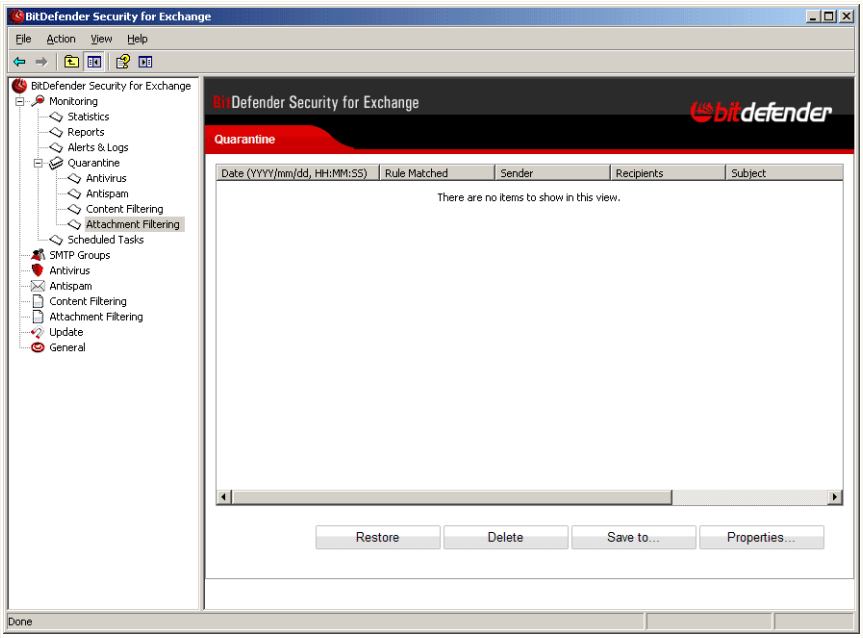
Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. In this way you can analyze the item and send it by mail.

To decrypt and deliver a quarantined message to its intended recipient, select the message and click **Restore**.

Note
To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 81).

9.5.4. Attachment Filtering Quarantine

Click **Attachment Filtering** in the tree menu (**Quarantine** module) to enter this section.



Attachment Filtering Quarantine

This is where you can see the messages that matched an Attachment Filtering rule and which were stored in the quarantine area.

For each quarantined message, the following information is provided: the date and time when it was quarantined, the matching rule, the mail address of the sender, the mail address of the recipients, the subject and the file name of the message.

Quarantined files are encrypted. In order to see an item from the quarantine area, select it and then click **Save to disk** to decrypt the file. In this way you can analyze the item and send it by mail.

To decrypt and deliver a quarantined message to its intended recipient, select the message and click **Restore**.

Note

To learn how to manage the quarantined files and the quarantine area, please refer to "*Managing Quarantine*" (p. 81).

9.5.5. Managing Quarantine

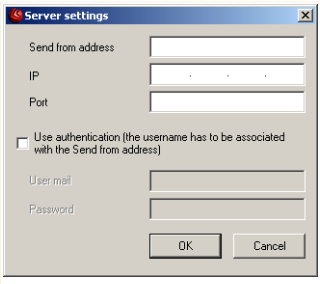
To manage the quarantined files and the quarantine areas, use the following buttons:

- **Restore** - decrypts selected quarantined messages from the Antispam, Content Filtering and Attachment Filtering quarantine areas and delivers them to their intended recipients. For more information, please refer to "*Restoring Quarantined Items*" (p. 81)
- **Delete** - deletes one or several selected files.
- **Save to** - decrypts the quarantined files and saves them to the disk. In this way you can see and analyze the quarantined item (message / attachment).
- **Properties** - configure the quarantine settings. For more information, please refer to "*Configuring Quarantine Properties*" (p. 83)

Restoring Quarantined Items

To decrypt and deliver messages from the Antispam, Content Filtering and Attachment Filtering quarantine areas to their intended recipients follow these steps:

1. Select one or more quarantined messages.
2. Click the **Restore** button.
3. If no SMTP server settings have been configured yet, you will be prompted to configure these settings. The following window will appear:



Server Settings

Specify the required SMTP server settings:

- **Send from address** - type the e-mail address that will appear in the sender field.

Important
Provide a valid e-mail address for the SMTP server, otherwise the server may decline to send an e-mail whose sender (e-mail address) is unknown to it.

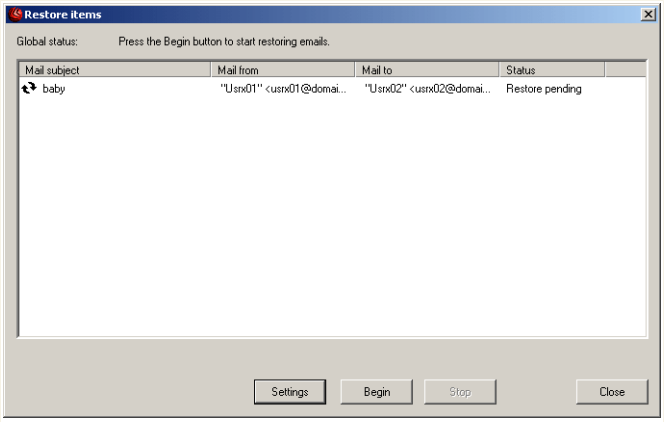
- **IP** - type the IP address used by the server.
- **Port** - type the port used by the server.

If the server used to send the messages requires authentication, select the **Use authentication** check box and enter the user name and password associated with the **Send from address**.

Note
NTLM authentication is not supported.

Click **OK** to save the changes and close the window.

4. You are ready to start restoring the messages. The following window will appear:



Restore Items

The e-mails selected for restoration are listed in this window. For each message, the subject, sender, recipient and restoration status are displayed. Click **Begin** to start delivering the messages.

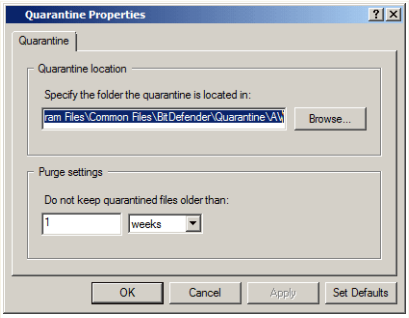
Once the process begins, you can abort it by clicking **Stop**.

To configure the server settings, click **Settings**. This will open the server settings window.

5. Wait for the restoration to complete and click **Close** to close the window.

Configuring Quarantine Properties

To set the location of the quarantine folder and configure the purge options, click the **Properties** button. The following window will appear:



Quarantine Properties

You can change the folder the quarantine is located in. Provide the new path in the edit field or click **Browse** to set a new location. The default location of the quarantine folders is: `C:\Program Files\BitDefender\BitDefender for Windows Servers Services\Quarantine`.

Note
The default quarantine folders for each component are the following:

- `C:\Program Files\BitDefender\BitDefender for Windows Servers Services\Quarantine\AV` for the Antivirus module.
- `C:\Program Files\BitDefender\BitDefender for Windows Servers Services\Quarantine\AS` for the Antispam module.
- `C:\Program Files\BitDefender\BitDefender for Windows Servers Services\Quarantine\CF` for the Content Filtering module.
- `C:\Program Files\BitDefender\BitDefender for Windows Servers Services\Quarantine\AF` for the Attachment Filtering module.

By default, quarantined files older than 90 days are automatically deleted. To change the time interval during which files are stored in the quarantine, type the number of hours / days / weeks / months in the corresponding field.

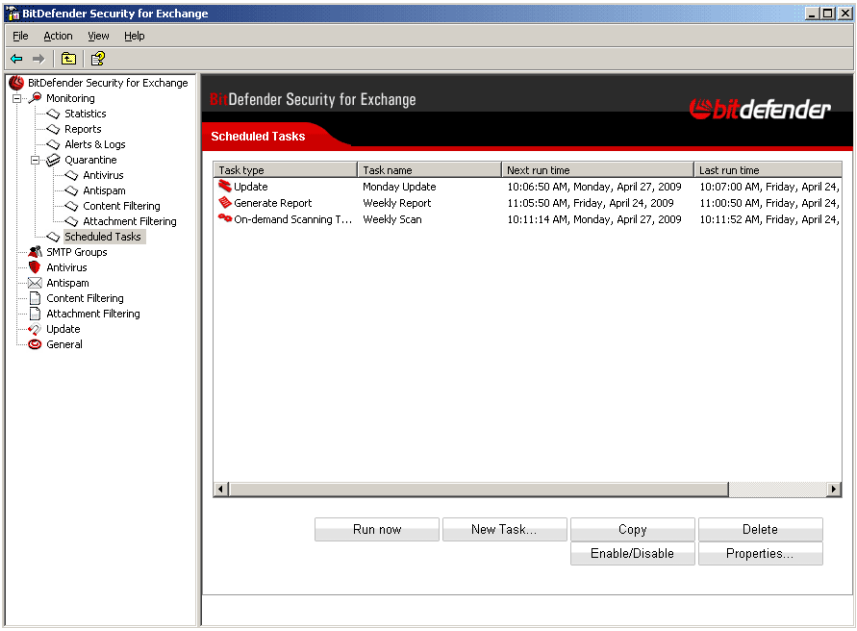
Click **OK** to save the changes and close the window. If you want to apply the default settings, click **Set Defaults**.

9.6. Scheduled Tasks

Scheduled tasks provide great flexibility and help perform administrative security tasks without increasing the workload and affecting the performance of the mail server. You can set BitDefender to perform specific tasks one-time only or on a regular basis according to a convenient schedule. You can schedule the following tasks:

- on-demand antivirus scanning of the Exchange databases (mailboxes and public folders).
- update processes.
- report generation tasks.

Click **Scheduled Tasks** in the tree menu (**Monitoring** module) to enter this section.



Scheduled Tasks

You can see all the existing scheduled tasks listed in the table. For each task, the following information is provided: the task type and name, the last time when it was performed, the next time it is scheduled to run and the status.

9.6.1. Managing Scheduled Tasks

To manage the scheduled tasks, use these buttons:

- **Run Now** - runs a selected scheduled task.
- **New Task** - launches a wizard that will help you create a new scheduled task.

> ***Note***
> The configuration wizard is different for each type of scheduled task.

- **Copy** - copies one or several selected scheduled tasks.

- **Delete** - deletes one or several selected scheduled tasks. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables / disables one or several selected scheduled tasks.
- **Properties** - opens the configuration window of a selected scheduled task, allowing you to modify it and to configure more advanced settings.

9.6.2. Update Tasks

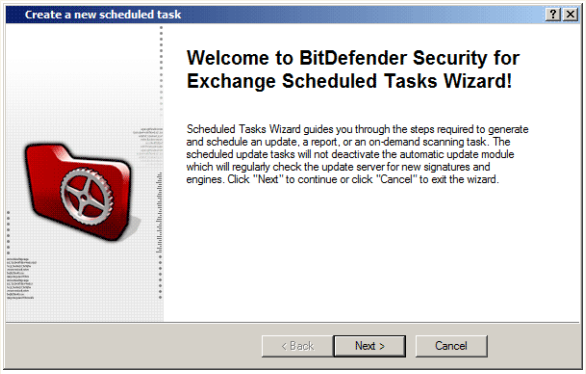
Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear and it will guide you through the process of creating a scheduled task.

Note
The scheduled update tasks will not deactivate the automatic update.

Follow these steps to schedule an update task:

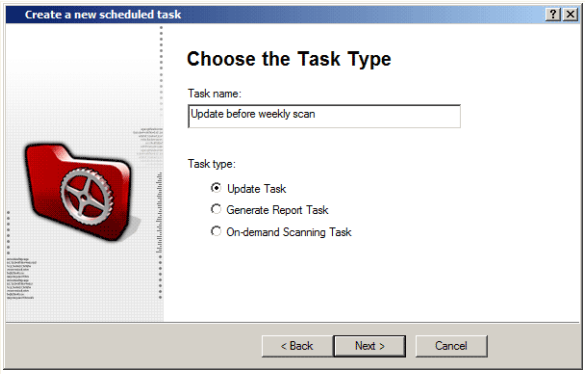
Step 1/4 - Welcome to the Scheduled Tasks Wizard


Create a new scheduled task
Welcome to BitDefender Security for Exchange Scheduled Tasks Wizard!
Scheduled Tasks Wizard guides you through the steps required to generate and schedule an update, a report, or an on-demand scanning task. The scheduled update tasks will not deactivate the automatic update module which will regularly check the update server for new signatures and engines. Click "Next" to continue or click "Cancel" to exit the wizard.
< Back
Next >
Cancel

Welcome

Click **Next**.

Step 2/4 - Select Task Type

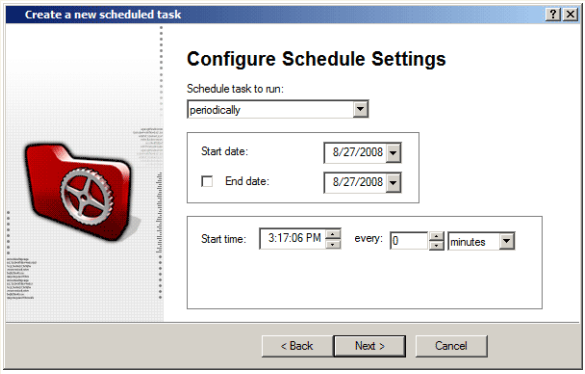


Select Task Type

Provide the task name and then select **Update Task**.

Click **Next**.

Step 3/4 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

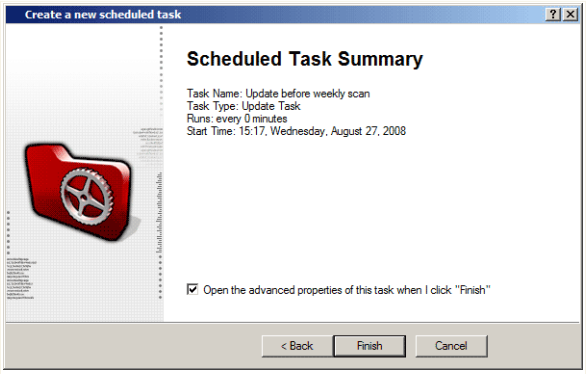
- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/4 - View Summary


Create a new scheduled task
Scheduled Task Summary
Task Name: Update before weekly scan
Task Type: Update Task
Runs: every 0 minutes
Start Time: 15:17, Wednesday, August 27, 2008
Open the advanced properties of this task when I click "Finish"
< Back
Finish
Cancel

View Summary

This window displays the task settings. You can make any changes by returning to the previous steps (click **Back**).

Select **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 89).

Click **Finish** to save the scheduled task.

Note
The task will appear in the Scheduled Tasks section.

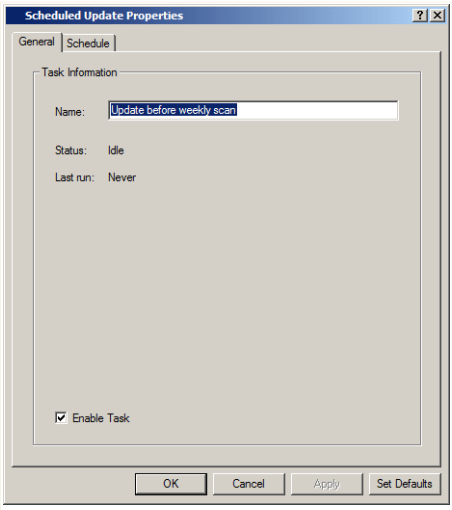
Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note
To open the configuration window, you can also select **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information

Open the configuration window to check general information.



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

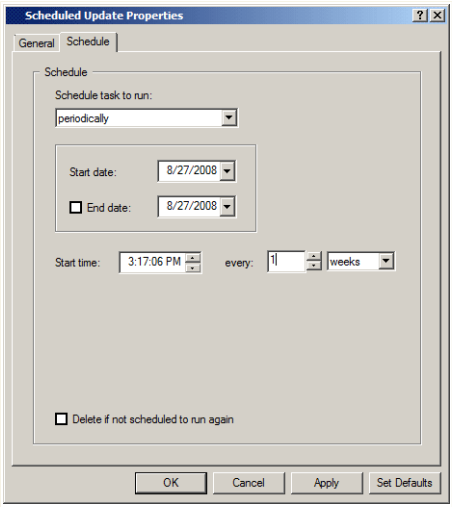
To enable the task, select **Enable Task**. Otherwise, clear this check box.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

Select **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

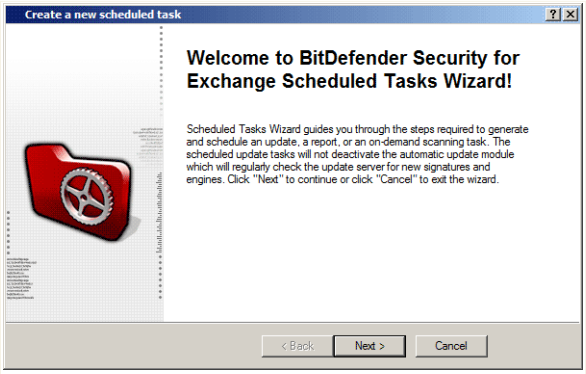
9.6.3. Generate Report Tasks

Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear and it will guide you through the process of creating a scheduled task.

Follow these steps to schedule a report generation task:

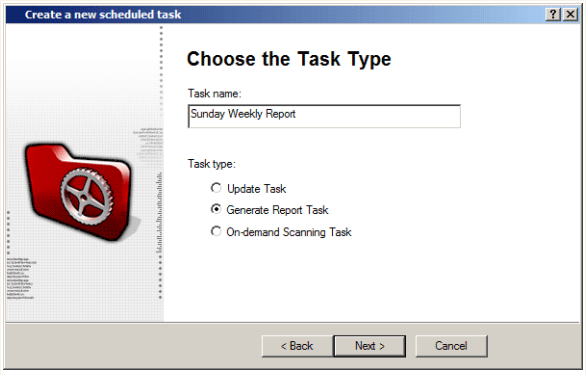
Step 1/7 - Welcome to the Scheduled Tasks Wizard


Create a new scheduled task
Welcome to BitDefender Security for Exchange Scheduled Tasks Wizard!
Scheduled Tasks Wizard guides you through the steps required to generate and schedule an update, a report, or an on-demand scanning task. The scheduled update tasks will not deactivate the automatic update module which will regularly check the update server for new signatures and engines. Click "Next" to continue or click "Cancel" to exit the wizard.
< Back
Next >
Cancel

Welcome

Click **Next**.

Step 2/7 - Select Task Type

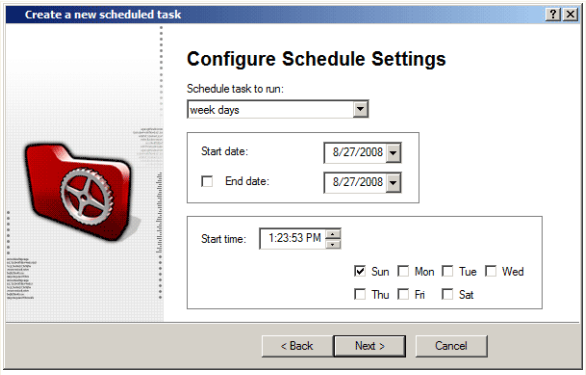


Select Task Type

Provide the task name and then select **Generate Report Task**.

Click **Next**.

Step 3/7 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

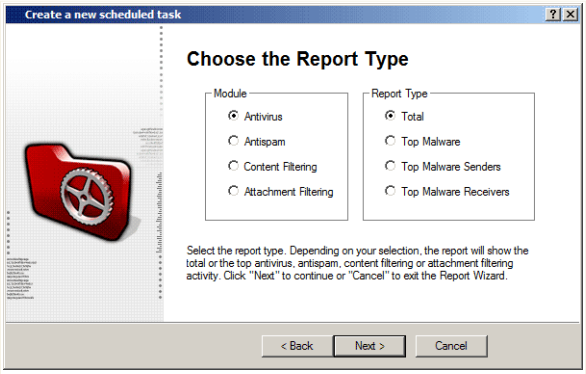
- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

1. Specify the start date in the **Start Date** field.
2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/7 - Select Report Type


Create a new scheduled task
Choose the Report Type
Module
Antivirus
Antispam
Content Filtering
Attachment Filtering
Report Type
Total
Top Malware
Top Malware Senders
Top Malware Receivers
Select the report type. Depending on your selection, the report will show the total or the top antivirus, antispam, content filtering or attachment filtering activity. Click "Next" to continue or "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Report Type

First, you must select the module the generated report is on: **Antivirus**, **Antispam**, **Content Filtering** and **Attachment Filtering**.

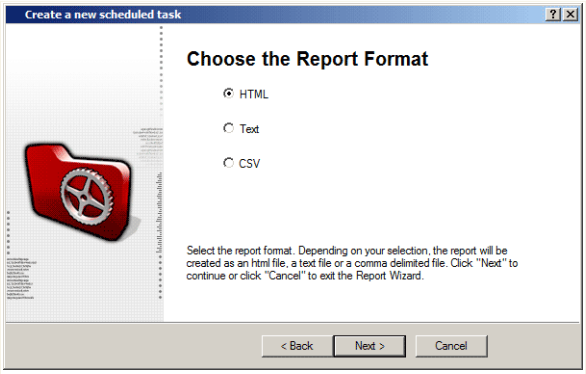
Then select one of the report types available for the module you have chosen.

Note
For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 52) section.

Depending on your choice, the report may contain a summary of or only specific data about the activity of a specified component.

Click **Next**.

Step 5/7 - Select Report Format

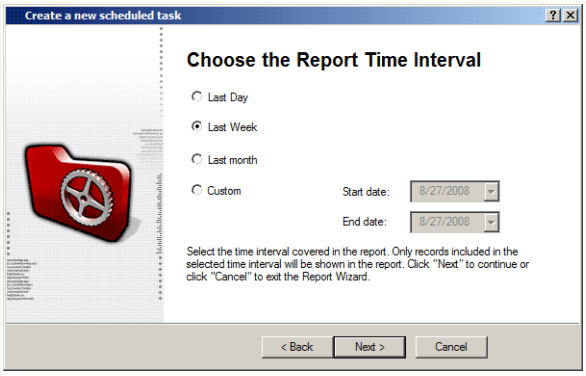

Create a new scheduled task
Choose the Report Format
HTML
Text
CSV
Select the report format. Depending on your selection, the report will be created as an html file, a text file or a comma delimited file. Click "Next" to continue or click "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Report Format

Select the format of the report file (**HTML**, **text** or **CSV**). Depending on your selection, the report will be created as an HTML, text or comma-separated values (CSV) file.

Click **Next**.

Step 6/7 - Select Time Interval


Create a new scheduled task
Choose the Report Time Interval
Last Day
Last Week
Last month
Custom
Start date:
8/27/2008
End date:
8/27/2008
Select the time interval covered in the report. Only records included in the selected time interval will be shown in the report. Click "Next" to continue or click "Cancel" to exit the Report Wizard.
< Back
Next >
Cancel

Select Time Interval

Select the time interval covered in the report:

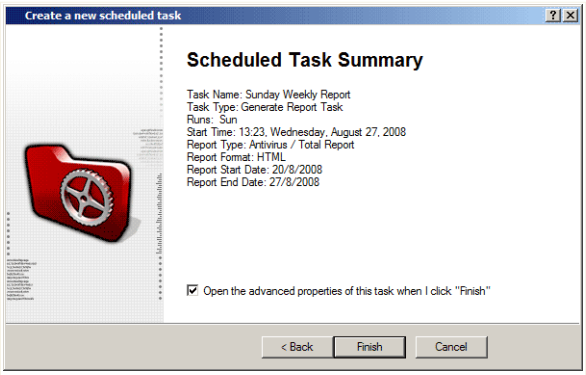
- **Last day**
- **Last week**
- **Last month**
- **Custom**

If you need information about the BitDefender activity related to a specific time interval, select **Custom** and specify the start and end date. To specify the start and end date, either click the numbers in the date field and enter new values or click **the arrow** to choose a date from the calendar.

Note
The date format is month/day/year.

Click **Next**.

Step 7/7 - View Summary


Create a new scheduled task
Scheduled Task Summary
Task Name: Sunday Weekly Report
Task Type: Generate Report Task
Runs: Sun
Start Time: 13:23, Wednesday, August 27, 2008
Report Type: Antivirus / Total Report
Report Format: HTML
Report Start Date: 20/8/2008
Report End Date: 27/8/2008
Open the advanced properties of this task when I click "Finish"
< Back
Finish
Cancel

View Summary

This window displays the task settings. You can make any changes by returning to the previous steps (click **Back**).

Select **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 98).

Click **Finish** to save the scheduled task.

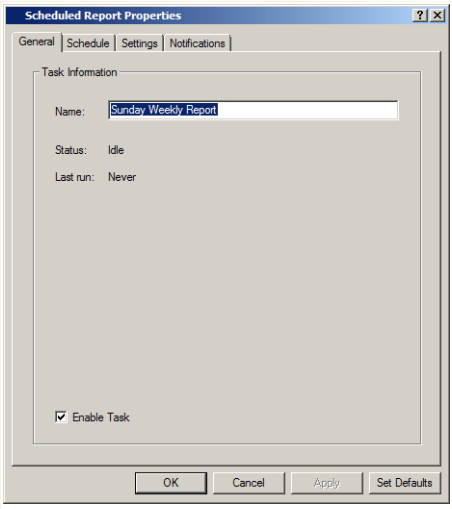
Note
The task will appear in the Scheduled Tasks section.

Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note
To open the configuration window, you can also select **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

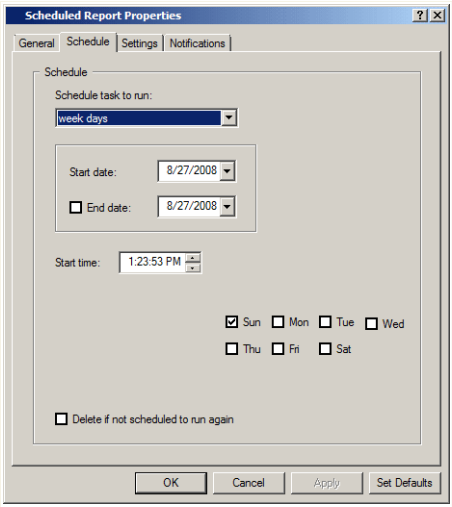
To enable the task, select **Enable Task**. Otherwise, clear this check box.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.

2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

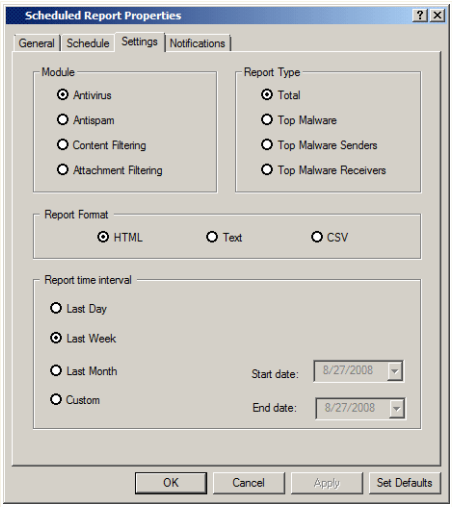
Select **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Settings

Click the **Settings** tab in the configuration window to modify the report settings.



Settings

Follow these steps to configure the report settings:

1. Choose on which module (Antivirus, Antispam, Content Filtering, Attachment Filtering) to generate the report.
2. Select one of the report types available for the previously specified module.

> ***Note***
> For more information on the available report types, please refer to the table presented at the beginning of the "*Reports*" (p. 52) section.

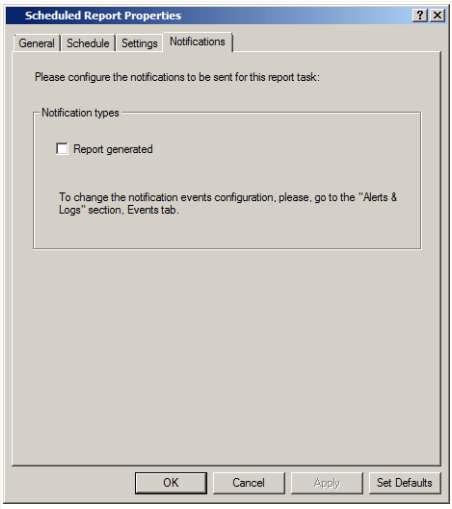
3. Select the format of the report file (**HTML**, **text** or **CSV**).
4. Select the time interval covered in the report:
   - **Last day**
   - **Last week**
   - **Last month**
   - **Custom**

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Notifications

Click the **Notifications** tab in the configuration window to configure notifications.



Notifications

Select **Report Generated** to enable notifications on report generation.

Note
To choose how to obtain information about the occurrence of this event, go to the **Alerts&Events** module, Events section and configure the corresponding event.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

9.6.4. On-demand Scanning Tasks

Scheduling Tasks

To create a new scheduled task, click **New task**. The configuration wizard will appear and it will guide you through the process of creating a scheduled task.

Follow these steps to schedule an on-demand scanning task:

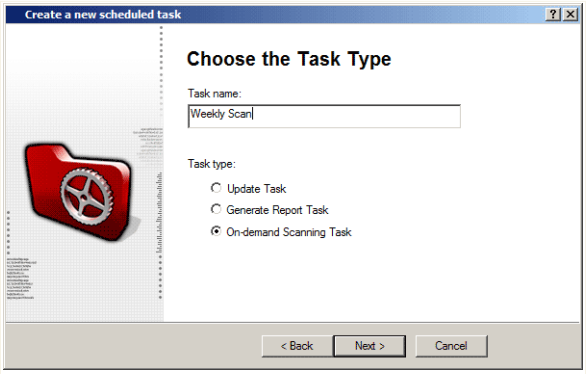
Step 1/7 - Welcome to the Scheduled Tasks Wizard

Create a new scheduled task
Welcome to BitDefender Security for Exchange Scheduled Tasks Wizard!
Scheduled Tasks Wizard guides you through the steps required to generate and schedule an update, a report, or an on-demand scanning task. The scheduled update tasks will not deactivate the automatic update module which will regularly check the update server for new signatures and engines. Click "Next" to continue or click "Cancel" to exit the wizard.
< Back
Next >
Cancel

Welcome

Click **Next**.

Step 2/7 - Select Task Type

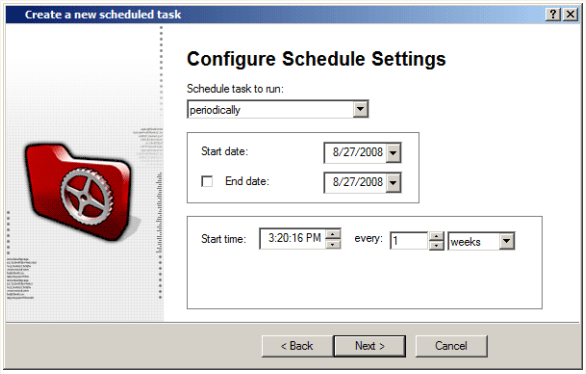


Select Task Type

Provide the task name and then select **On-demand Scanning Task**.

Click **Next**.

Step 3/7 - Configure Schedule



Run Task Periodically

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

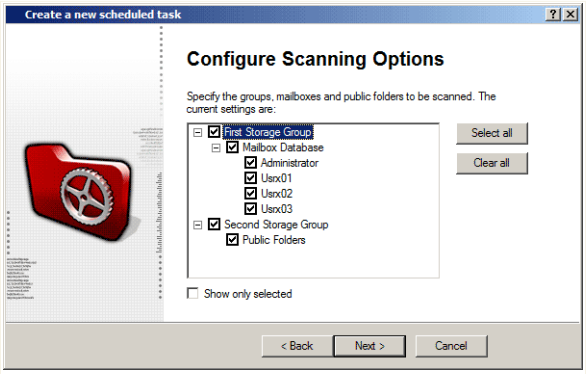
- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

Click **Next**.

Step 4/7 - Select Scan Target



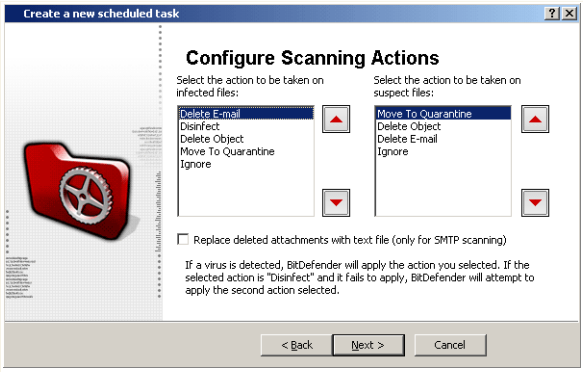
Select Scan Target

Select the check boxes corresponding to the items (groups, mailboxes and public folders) you want to be scanned. If you want to scan all the Exchange databases (mailboxes and public folders), just click **Select All**.

To clear all check boxes and start a new selection, click **Clear All**. You can select **Show only selected** to display only the items to be scanned.

Click **Next**.

Step 5/7 - Set Actions


Create a new scheduled task
Configure Scanning Actions
Select the action to be taken on infected files:
Delete E-mail
Disinfect
Delete Object
Move To Quarantine
Ignore
Select the action to be taken on suspect files:
Move To Quarantine
Delete Object
Delete E-mail
Ignore
Replace deleted attachments with text file (only for SMTP scanning)
If a virus is detected, BitDefender will apply the action you selected. If the selected action is "Disinfect" and it fails to apply, BitDefender will attempt to apply the second action selected.
< Back
Next >
Cancel

Set Actions

Different actions can be configured for the infected and suspect objects detected by BitDefender. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

You can change the order in which actions are to be applied. Select an action and click or to move it up or down in the list.

Actions for infected objects. The following actions are available for infected objects:

Action	Description
Disinfect	The infected message is disinfected.
Move to Quarantine	The infected object (mail body / attachment / public file) is moved to the quarantine folder.
Delete object	The infected object (mail body / attachment / public file) is deleted.
Delete e-mail	The infected message is deleted.
Ignore	The infected message is delivered in full to its recipients.

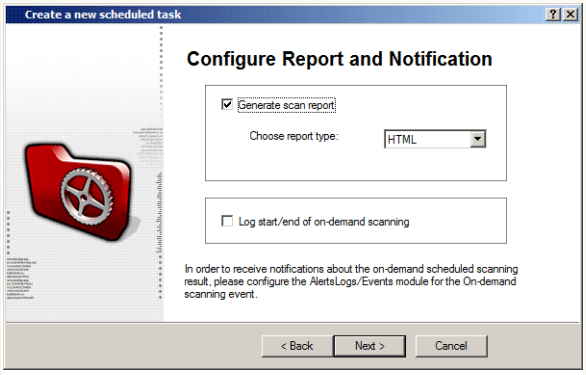
Actions for suspect objects. The following actions are available for suspect objects:

Action	Description
Move to Quarantine	The suspect object (mail body / attachment / public file) is moved to the quarantine folder.
Delete object	The suspect object (mail body / attachment / public file) is deleted.
Delete e-mail	The suspect message is deleted.
Ignore	The suspect message is delivered in full to its recipients.

In addition, BitDefender can replace the infected or suspect objects that are deleted or moved to quarantine with an explanatory text. To enable this option, select the **Replace deleted attachments with text file (only SMTP scanning)** check box.

Click **Next**.

Step 6/7 - Configure Notifications Options


Create a new scheduled task
Configure Report and Notification
Generate scan report
Choose report type:
HTML
Log start/end of on-demand scanning
In order to receive notifications about the on-demand scheduled scanning result, please configure the Alerts/Logs/Events module for the On-demand scanning event.
< Back
Next >
Cancel

Configure Notifications Options

Configure Report Options

Select **Generate Scan Report** to generate a report for the on-demand scan. By default, the report file is saved in: `C:\Program Files\BitDefender\BitDefender Security for Exchange\Reports`.

The report can be generated in HTML, text or CSV format. You can choose the format of the report file from the menu.

Note
To view the report file, at the end of the scanning, open the configuration window (select the task and click **Properties**) and then click **View Log**.

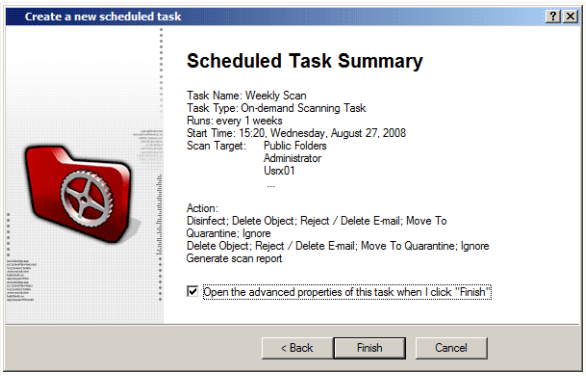
Log Scanning

Select **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

Note
The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Click **Next**.

Step 7/7 - View Summary


Create a new scheduled task
Scheduled Task Summary
Task Name: Weekly Scan
Task Type: On-demand Scanning Task
Runs: every 1 weeks
Start Time: 15:20, Wednesday, August 27, 2008
Scan Target: Public Folders
Administrator
Usrx01
...
Action:
Disinfect; Delete Object; Reject / Delete E-mail; Move To Quarantine; Ignore
Delete Object; Reject / Delete E-mail; Move To Quarantine; Ignore
Generate scan report
Open the advanced properties of this task when I click "Finish"
< Back
Finish
Cancel

View Summary

This window displays the task settings. You can make any changes by returning to the previous steps (click **Back**).

Select **Open the advanced properties of this task when I click "Finish"** if you want the **Properties** window of this task to be opened after you complete the wizard. In this window you can modify the task and configure more advanced settings. For more information, please refer to "*Configuring Properties*" (p. 110).

Click **Finish** to save the scheduled task.

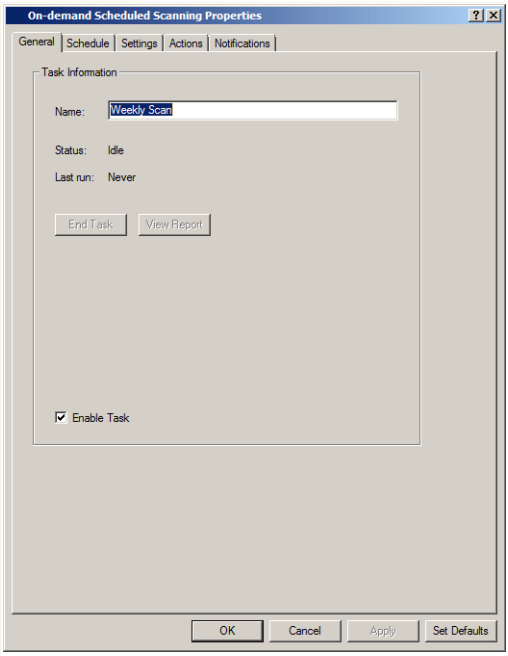
Note
The task will appear in the Scheduled Tasks section.

Configuring Properties

In order to modify an existing scheduled task or to configure more advanced settings, unavailable in the configuration wizard, just double-click the task or select it and click **Properties**. The configuration window will appear.

Note
To open the configuration window, you can also select **Open the advanced properties of this task when I click "Finish"** in the last step of the wizard.

Viewing General Information



General

You can see general information about the task (the name, the status, the last time when the task ran). If you want to change the task name, enter a new name in the corresponding field.

If the task is running, you can end the scanning process by clicking **End Task**.

To see the report file on the last task execution, click **View Log**.

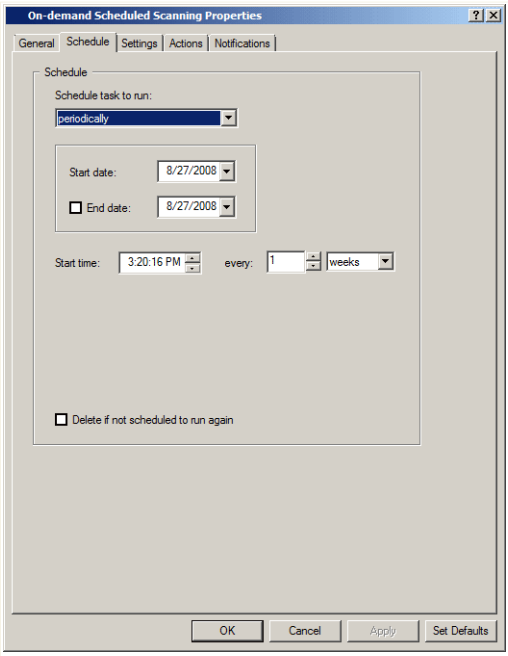
To enable the task, select **Enable Task**. Otherwise, clear this check box.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Modifying Schedule

Click the **Schedule** tab in the configuration window to modify the schedule.



Schedule

Specify the task schedule.

You must choose one of the following options from the menu:

- **Once** - to run the task one time only, at a given moment.

  Specify the start date and time in the **Start Date / Start Time** fields.

- **Periodically** - to run the task periodically, at certain time intervals (minutes, hours, days, weeks, months, years), starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.

2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in the corresponding field.
3. Specify the start time in the **Start Time** field.
4. Specify the task frequency by specifying the number of minutes / hours / days / weeks / months / years between two successive occurrences of such task, in the corresponding field.

- **Week Days** - to run the task repeatedly only in certain days of the week starting with a specified date and time.

  To configure the necessary settings, follow these steps:

  1. Specify the start date in the **Start Date** field.
  2. If you want to run the task repeatedly until a certain date, check **End Date** and specify the end date in corresponding field.
  3. Specify the start time in the **Start Time** field.
  4. Specify the day or days of the week on which the task should be run.

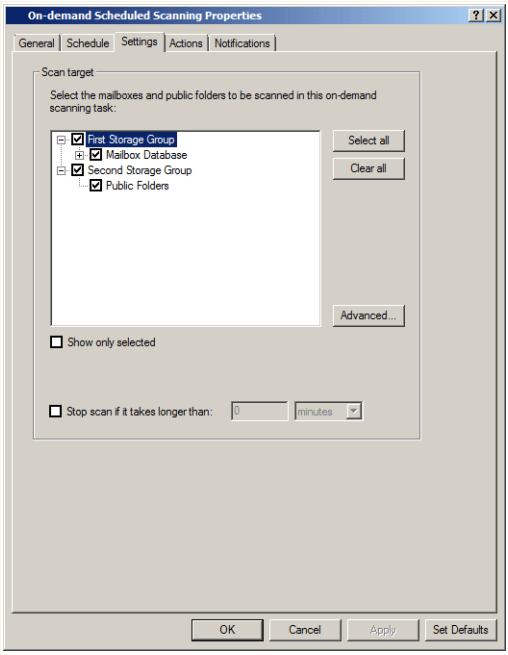
Select **Delete if not scheduled to run again** to delete the task after its last execution.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Settings

Click the **Settings** tab in the configuration window to modify the task settings.



Settings

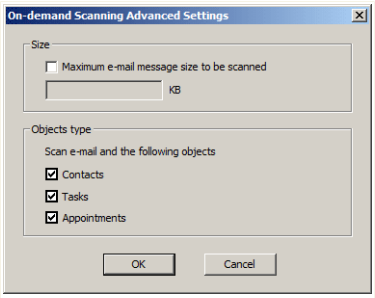
Select Scan Target

Select the check boxes corresponding to the items (groups, mailboxes and public folders) you want to be scanned. If you want to scan all the Exchange databases (mailboxes and public folders), just click **Select All**.

To clear all check boxes and start a new selection, click **Clear All**. You can select **Show only selected** to display only the items to be scanned.

Set Advanced Settings

To set advanced scan settings click **Advanced**. A new window will appear.



Advanced Scan Settings

If you do not want to scan messages that exceed a certain size limit, select **Maximum mail size to be scanned** and provide the size limit in the corresponding field.

Beside messages, you can select other objects to be scanned: **Contacts**, **Tasks** and **Appointments**.

Click **OK** to save changes and close the window.

Limit Scanning Time

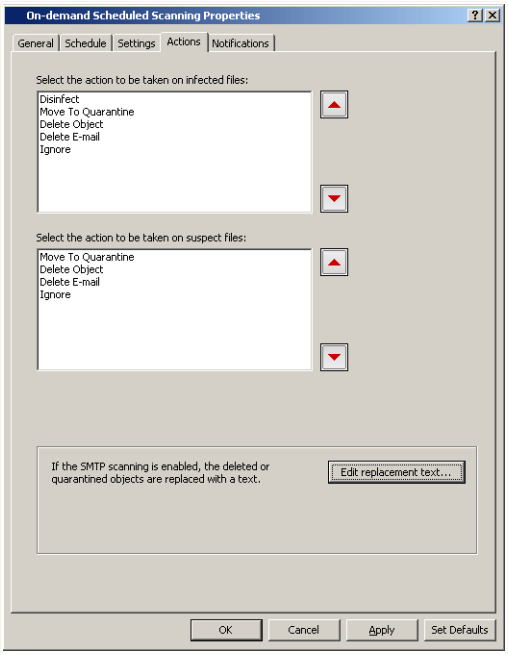
If you want to limit the scanning time, select **Stop scan if it takes longer than** and specify the number of minutes or hours.

Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

Configuring Actions

Click the **Actions** tab and specify the actions to be taken on infected and suspect objects.



Actions

Different actions can be configured for the infected and suspect objects detected by BitDefender. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

You can change the order in which actions are to be applied. Select an action and click or to move it up or down in the list.

Actions for infected objects. The following actions are available for infected objects:

Action	*Description*
Disinfect	The infected message is disinfected.

Action	Description
Delete object	The infected object (mail body / attachment / public file) is deleted.
Delete e-mail	The infected message is deleted.
Move to Quarantine	The infected object (mail body / attachment / public file) is moved to the quarantine folder.
Ignore	The infected message is delivered in full to its recipients.

Actions for suspect objects. The following actions are available for suspect objects:

Action	Description
Delete object	The suspect object (mail body / attachment / public file) is deleted.
Delete e-mail	The suspect message is deleted.
Move to Quarantine	The suspect object (mail body / attachment / public file) is moved to the quarantine folder.
Ignore	The suspect message is delivered in full to its recipients.

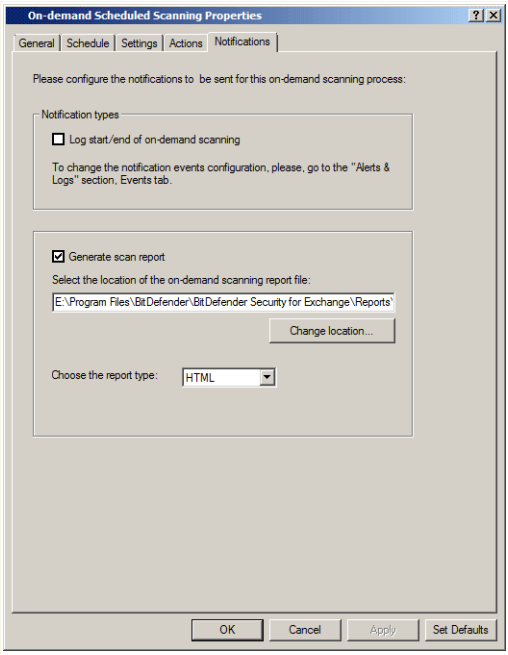
BitDefender replaces the infected or suspect objects that are deleted or moved to quarantine with an explanatory text.

To edit the text to be delivered instead of such objects, follow these steps:

1. Click **Edit replacement text...**. A new window will appear.
2. Do any or both of the following:
   - Select **Infected file replaced** and type in the edit box the text to be delivered instead of the infected or suspect objects deleted.
   - Select **Infected file quarantined** and type in the edit box the text to be delivered instead of the infected or suspect objects moved to quarantine.

Configuring Notifications

Click the **Notifications** tab in the configuration window to configure the notifications.



Notifications

Log Scanning

Select **Log start/end of on-demand scanning** to record the start and the end of the process in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Configure Report Settings

Select **Generate Scan Report** to generate a report for the on-demand scan. By default, the report file is saved in: `C:\Program Files\BitDefender\BitDefender Security for Exchange\Reports`. To change this location click **Change location**.

The report can be generated in HTML, text or CSV format. You can choose the format of the report file from the menu.

Note
To view the report file, at the end of the scanning process, open the configuration window (select the task and click **Properties**) and then click **View Log**.

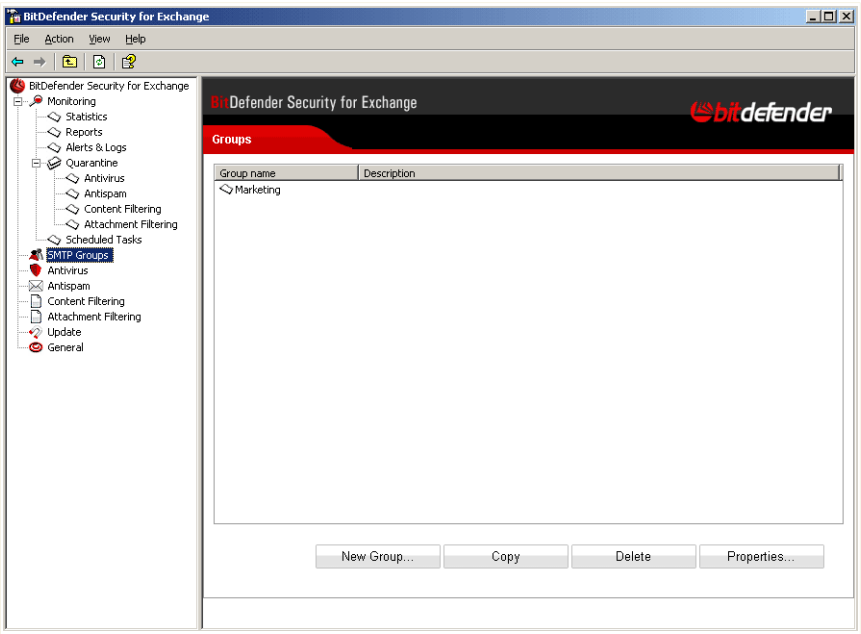
Click **Apply** to save the changes. If you want to save the changes and close the configuration window, click **OK**.

If you want to close the configuration window without making any changes, click **Cancel**.

10. SMTP Groups

BitDefender allows creating user groups, in order to apply different scanning and filtering policies for different user categories. For example, you can create appropriate policies for the IT department, for the sales team or for the managers of your company.

To create new user groups or manage existing groups, click **SMTP Groups** in the tree menu.



Groups

You can see all the existing groups listed in the table along with their description.

10.1. Managing Groups

To manage the groups, use these buttons:

- **New Group** - creates a new group. You will have to configure the group before it appears in the table.
- **Copy** - copies one or several selected groups.
- **Delete** - deletes one or several selected groups. You will have to confirm your choice by clicking **Yes**.
- **Properties** - opens the configuration window of a selected group, allowing you to configure it. To learn how to configure the group, please refer to "*Configuring Groups*" (p. 121).

10.2. Creating Groups

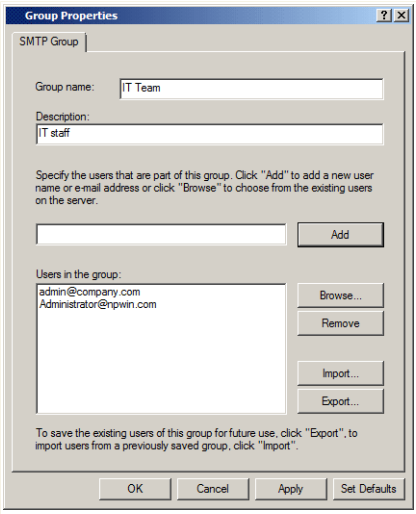
To create a group, choose one of the following methods:

- copy an existing group and click **Properties** to modify it.
- click **New Group** and configure the new group.

In both cases, a configuration window will appear. Next, you must configure the group.

10.3. Configuring Groups

Open the configuration window (select the group and click **Properties**).

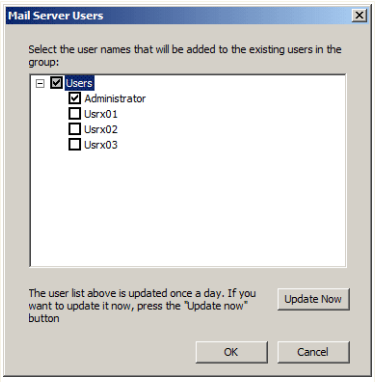

Group Properties
SMTP Group
Group name:
IT Team
Description:
IT staff
Specify the users that are part of this group. Click "Add" to add a new user name or e-mail address or click "Browse" to choose from the existing users on the server.
Add
Users in the group:
admin@company.com
Administrator@npwin.com
Browse...
Remove
Import...
Export...
To save the existing users of this group for future use, click "Export", to import users from a previously saved group, click "Import".
OK
Cancel
Apply
Set Defaults

Group Properties

To configure the group follow these steps:

1. **Identify the new group.** Provide the group name and, optionally, the group description in the corresponding fields.
2. **Add users to the new group.**
   - Provide the e-mail address in the corresponding field and click **Add**.
   - Add users from the Active Directory user list.

     Click **Browse** to search users in the Active Directory user list. A new window will appear.


Mail Server Users
Select the user names that will be added to the existing users in the group:
Users
Administrator
Usrx01
Usrx02
Usrx03
The user list above is updated once a day. If you want to update it now, press the "Update now" button
Update Now
OK
Cancel

Browse for Users (Groups)

You can see the list of all the users from Active Directory that have an SMTP address assigned. The list structure is the one from Active Directory.

The user list is automatically updated once a day. To update the list, click **Update Now**.

Click the box labeled with "+" to show all items contained by an object or the box labeled with "-" to hide the items contained by an object.

Select the items you want to add to the new group and click **OK**.

- Import e-mail addresses from a txt file. Click **Import**, select the file and then click **Open** to add the addresses from the file to the group.

To remove one or several items from the list, select them, click **Remove** and then **Yes** to confirm your choice.

You can export the list to a txt file in order to use it when creating other groups. Click **Export** and save the file to the desired location.

3. Click **OK** to save the changes and close the configuration window.

11. Antivirus

The Antivirus module protects the Exchange server against viruses, spyware and riskware, and it ensures that users do not access infected e-mails. It detects infected or suspect messages and attempts to disinfect them or isolates the infection, according to the specified actions.

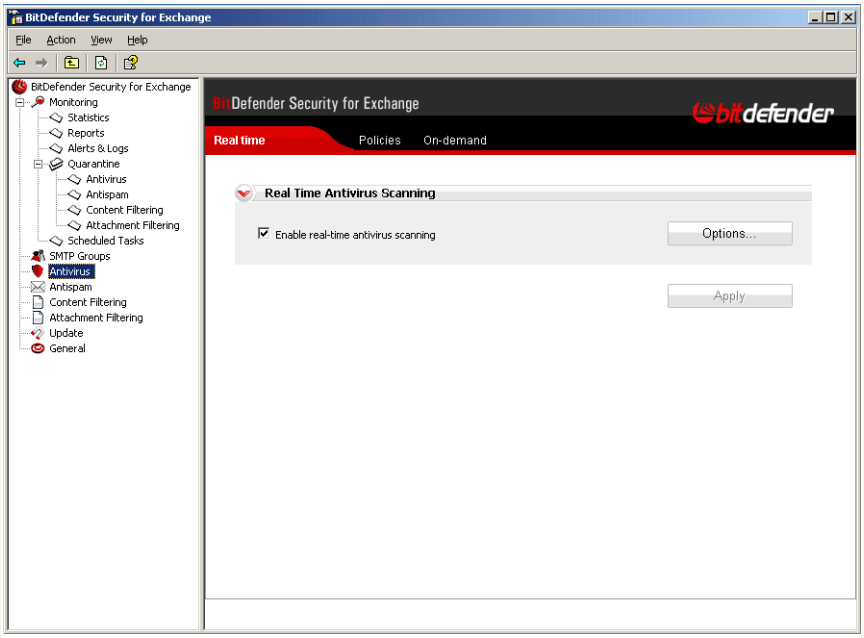
The default settings can be managed in the Policies tab through the default rule. Additionally, you can create scanning policies for different user groups.

You can optimize mail delivery by using background scanning during off working hours. To enable background scanning, go to the Real-time tab, click **Advanced** and select **Enable background scanning**. Do not forget to disable background scanning when the work hours begin, as it takes up system resources.

When needed, you can configure and initiate the on-demand scanning of the Exchange databases (mailboxes and public folders). To do this, go to the On-demand tab. Please note that on-demand scanning slows down the system.

11.1. Real-time Antivirus Protection

Click **Antivirus** in the tree menu to enter this section.



Real-time Antivirus Protection

This is where you can enable real-time protection and configure advanced antivirus settings.

If you want the real-time antivirus protection to be enabled, select **Enable real-time antivirus scanning**. Otherwise, clear the check box. Click **Apply** to save the changes.

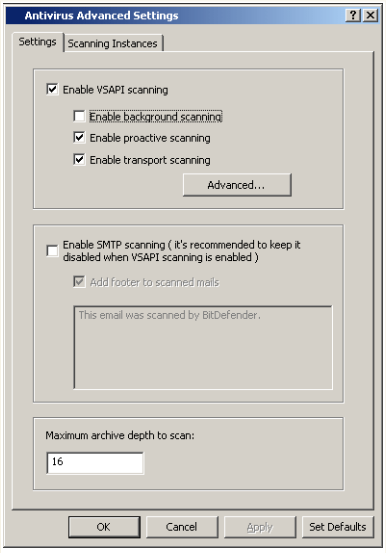
Note

In order to configure the antivirus scanning options for all of the incoming mail traffic or to create different scanning policies based on user groups, go to the Policies section.

11.1.1. Configuring Advanced Antivirus Settings

Several advanced settings concerning the scanning process can be configured. These settings are applied regardless of the policy.

Click **Options** to open the configuration window of the advanced antivirus settings.



Advanced Antivirus Settings

In this window you can configure VSAPI scanning and SMTP scanning settings, as well as the number of scanning instances and the maximum archive depth to scan.

VSAPI Scanning Settings

Select the **Enable VSAPI scanning** check box to enable VSAPI based antivirus scanning. The antivirus scanning at VSAPI level can be done through three additional scanning methods, intended to optimize the overall scanning process: background, proactive and transport scanning.

- **Enable background scanning** - select this option if you want background scanning to be enabled.

Background scanning means scanning all folders with a low priority. When an object that has been checked by the background scanning is requested, it will not be scanned again unless a virus definition update has been made. Therefore, enabling this scan method optimizes the overall scanning process.

To perform background scanning of the messages and attachments, the Information Store will use one thread per database, running at low priority. Once the background scanning is completed, the thread is terminated. This thread is not part of the global virus-scanning thread pool used for on-access scanning.

- **Enable proactive scanning** - select this option if you want proactive scanning to be enabled.

  Proactive scanning means that when a message is submitted to the information store, either via a client or a transport agent, it is placed in the global scanning queue with a low priority. If and when threads are available in the thread pool and no high priority item remains to be scanned, each item with the low priority is submitted for scanning. Therefore, enabling this scan method optimizes the overall scanning process.

  If an item is on the low priority list and a client attempts to access the message, the item will be marked as high priority. Also, it will be removed from the low priority list and another low priority item will take its place.

  Note
  We recommend you to keep this setting enabled as it prevents the overloading of the scanning engine.

- **Enable transport scanning** - select this option if you want transport scanning to be enabled.

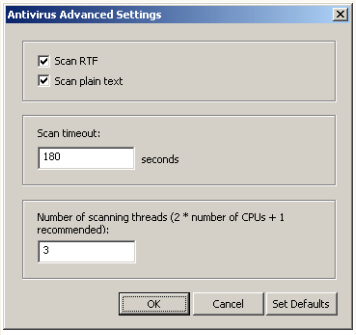
  Note
  Transport scanning is available only on MS Exchange Server 2003!

  Transport scanning means that messages are scanned at the transport level. This prevents infected messages from entering the Exchange mailboxes.

  The messages entering the Exchange store are intercepted by the VS API interface and scanned by BitDefender. After being scanned, the messages are submitted again to the transport engine which will deliver them to their destination. Any message scanned at the gateway will be rescanned on the back-end server.

Note
We recommend enabling transport scanning only when BitDefender Security for Exchange is installed on a gateway.

Additional options are available by clicking the **Advanced** button.



Advanced VSAPI settings

- **Scan RTF** - select this option if you want the body messages in Rich Text Format (RTF) to be scanned.
- **Scan Plain Text** - select this option if you want the body messages in plain text format to be scanned.
- **Scan Timeout** - type in the corresponding field the maximum time allocated to scan an object. If the scanning process is not completed before the timeout interval, an error is returned and access to the object is denied.
- **Number of scanning threads** - type in the corresponding field the maximum number of scanning threads to be used. The recommended number can be computed in this way: `2*number of CPU+1`.

Click **OK** to save the changes. If you want to restore the default settings, click **Set Defaults**.

SMTP Scanning Options

Select the **Enable SMTP scanning** check box to enable SMTP based antivirus scanning.

If SMTP scanning is enabled, BitDefender can add a footer to all scanned mails. Select the **Add footer to scanned emails** check box to activate this option and type the desired text in the text box below.

Maximum Archive Depth To Scan

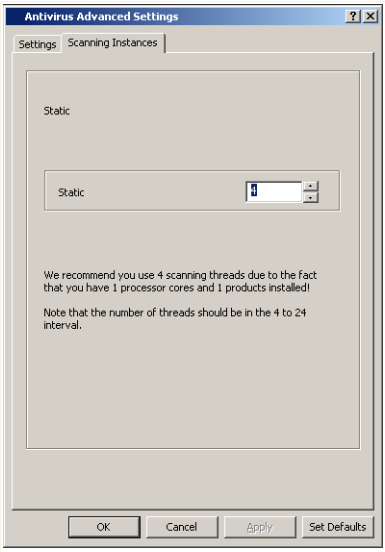
Archives can contain other archives. It is possible to find files with multiple archive levels. If there are too many such levels, the scanning process can take longer, affecting the performance of the server. It is advisable to set a maximum level up to which the archives are to be scanned.

To set the maximum archive depth to scan, type the desired level in the corresponding box. The default archive depth scanned is 16.

Click **OK** to save the changes. If you want to restore the default settings, click **Set Defaults**.

Scanning Instances

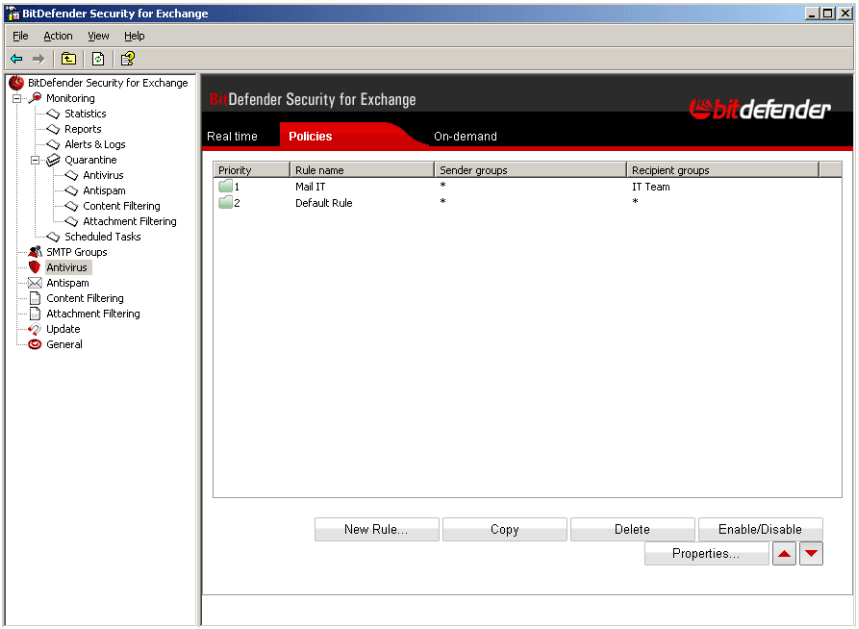
Based on the system configuration and on the number of BitDefender products you have chosen to install, BitDefender computes an optimal number of scanning instances. Though not recommended, you may change this value for systems with powerful multicore CPUs to speed up scanning.


Antivirus Advanced Settings
Settings
Scanning Instances
Static
Static
4
We recommend you use 4 scanning threads due to the fact that you have 1 processor cores and 1 products installed!
Note that the number of threads should be in the 4 to 24 interval.
OK
Cancel
Apply
Set Defaults

Scanning Instances

11.2. Policies

Click **Antivirus** in the tree menu and then the **Policies** tab to enter this section.



Policies

This is where you can configure the rules of the real-time antivirus scanning.

11.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and recipients it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the antivirus scanning options specified by that rule.

Please note that messages can be scanned before the rule is applied, by the transport (only for MS Exchange Server 2003), proactive or background scanning, regardless of the policy.

- If the message was not scanned before the client's request, it is scanned according to the rule.
- If the message was checked before by proactive or background scanning and no update was performed in the meantime, the message is delivered without being scanned according to the rule.
- If the message was checked before by proactive or background scanning but an update was performed in the meantime, the message is scanned according to the rule.
- **Only for MS Exchange Server 2003!** If the message was previously scanned at transport level, it is also scanned according to the rule.

For more information, please refer to "*Configuring Advanced Antivirus Settings*" (p. 126).

Default Rule. There is one rule created by default that manages the global real-time antivirus scanning settings. You can neither copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different antivirus policies, add new rules. In this way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one / several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables or disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 133).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

11.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

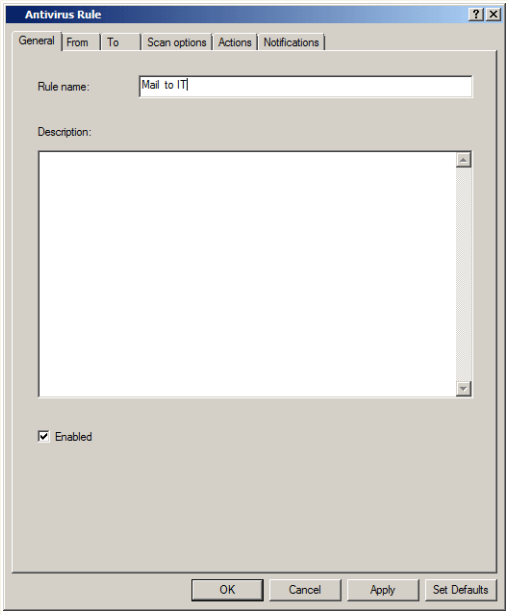
In both cases, a new window will appear. Next, you must configure or modify the rule.

11.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/6 - Provide General Data

Open the configuration window and provide general data for the rule.



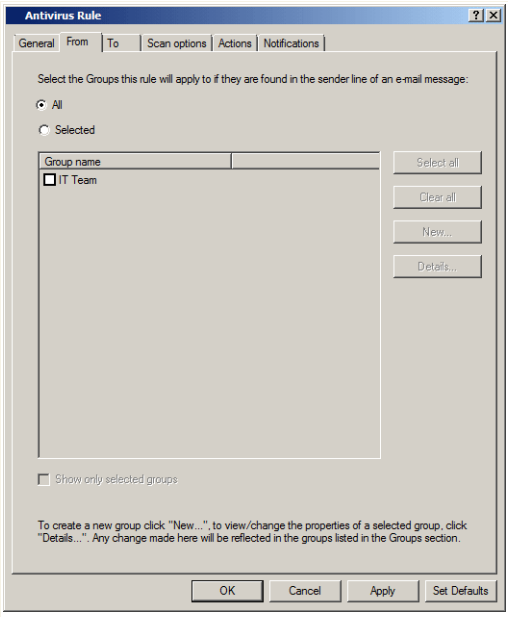
General

Provide the rule name and, optionally, the rule description.

To enable the rule, select **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/6 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to senders from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

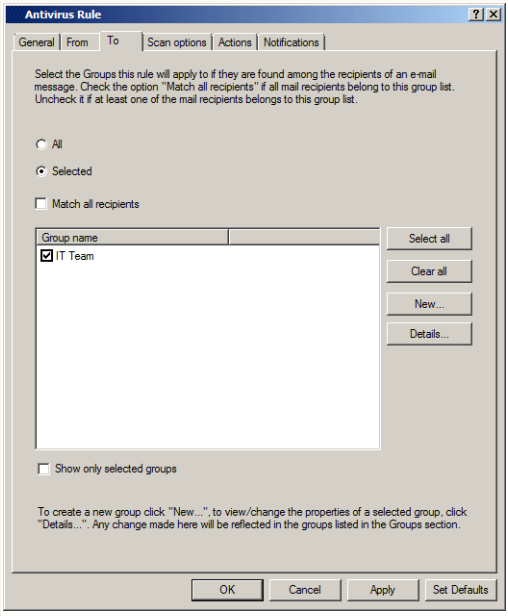
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 3/6 - Select Recipients Groups

Click the **To** tab and select the groups of recipients the rule applies to.


Antivirus Rule
General
From
To
Scan options
Actions
Notifications
Select the Groups this rule will apply to if they are found among the recipients of an e-mail message. Check the option "Match all recipients" if all mail recipients belong to this group list. Uncheck it if at least one of the mail recipients belongs to this group list.
All
Selected
Match all recipients
Group name
IT Team
Select all
Clear all
New...
Details...
Show only selected groups
To create a new group click "New...", to view/change the properties of a selected group, click "Details...". Any change made here will be reflected in the groups listed in the Groups section.
OK
Cancel
Apply
Set Defaults

Recipients Groups

The following options are available:

- **All** - the rule applies to all recipients, no matter if they belong to a group or not.
- **Selected** - the rule applies only to recipients from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all recipients** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note
The addresses in the **Cc** and **Bcc** fields also count as recipients.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

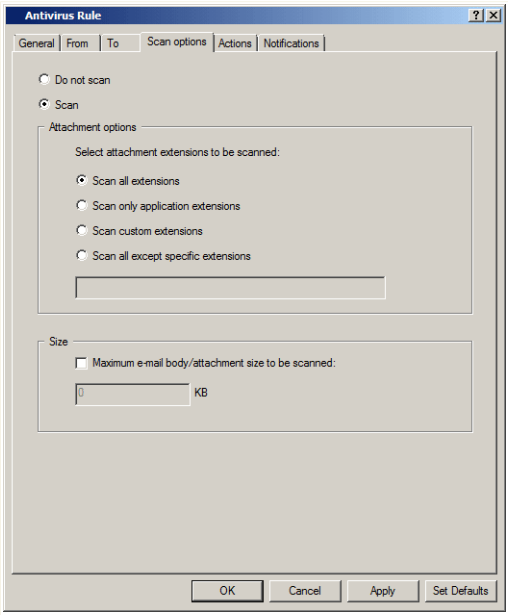
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 4/6 - Configure Scan Options

Click the **Scan Options** tab and configure the scan options for the messages matching this policy.



Scan Options

If you do not want the messages to be scanned for malware, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned for malware using the settings configured for this policy. You can specify:

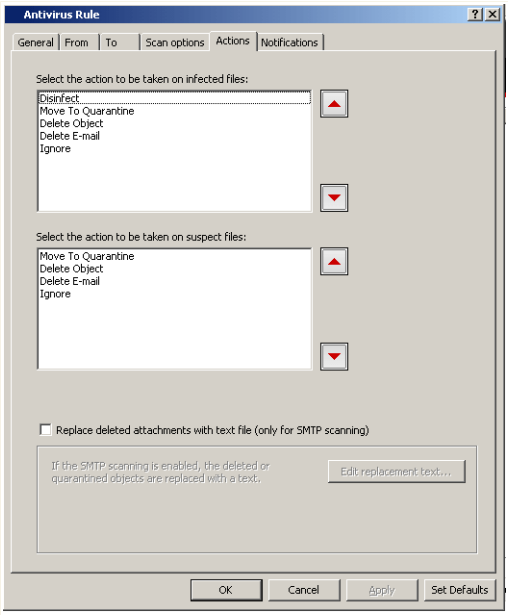
- **Attachment extensions to be scanned** - select one of the following options in order to scan attachments depending on their extension.

Option	Description
Scan all extensions	All mail attachments are scanned, regardless of their extension.
Scan only application extensions	Only the attachments containing applications are scanned. This category is limited to files with the following extensions: .exe; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .bat; .drv; .cpl.
Scan custom extensions	Only the attachments having the specified extensions are scanned. Provide the specific extensions in the edit field. These extensions must be separated by ";".
Scan all except specific extensions	All attachments except those having the specified extensions are scanned. Provide the extensions excepted from scanning in the edit field. These extensions must be separated by ";".

- **Maximum mail body / attachment size to be scanned** - select this option if you want to specify a size limit for the mail body or for the attachments to be scanned. Provide the size limit in the edit field.

Step 5/6 - Set Actions

Click the **Actions** tab and specify the actions to be taken on infected and suspect objects.



Actions

Different actions can be configured for the infected and suspect objects detected by BitDefender. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

You can change the order in which actions are to be applied. Select an action and click or to move it up or down in the list.

Actions for infected objects. The following actions are available for infected objects:

Action	*Description*
Disinfect	Removes the malware code from the infected message.
Move to Quarantine	The infected object (mail body / attachment) is moved to the quarantine folder.

Action	Description
Delete object	The infected object (mail body / attachment) is deleted.
Delete e-mail	The infected message is deleted.
Ignore	The infected message is delivered in full to its recipients.

Note
The **Delete e-mail** action does not work on Exchange 2000 VSAPI scanning, it only works on Exchange 2000 SMTP scanning.

Actions for suspect objects. The following actions are available for suspect objects:

Action	Description
Move to Quarantine	The suspect object (mail body / attachment) is moved to the quarantine folder.
Delete object	The suspect object (mail body / attachment) is deleted.
Delete e-mail	The suspect message is deleted.
Ignore	The suspect message is delivered in full to its recipients.

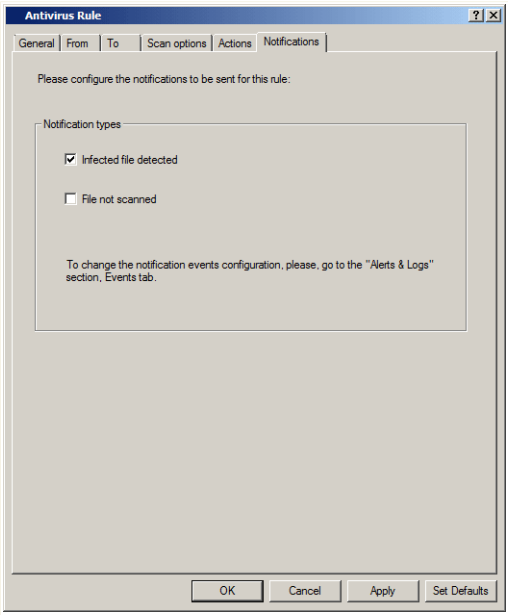
On the Exchange servers installed with the Mailbox role, the objects that are deleted or moved to quarantine can be replaced with a text.

To enable this option, select the **Replace deleted attachments with text file (only for SMTP scanning)** check box. To change the text to be delivered instead of such objects, follow these steps:

1. Click **Edit Replacement text...**. A new window will appear.
2. Do any or both of the following:
   - Select **Infected file replaced** and type in the edit box the text to be delivered instead of the infected or suspect objects deleted.
   - Select **Infected file quarantined** and type in the edit box the text to be delivered instead of the infected or suspect objects moved to quarantine.
3. Click **OK** to save the changes and close the window.

Step 6/6 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when infected messages are detected or files cannot be scanned.



Notifications

Select the events for which to issue notifications:

- **Infected file detected** - when an infected file was detected.
- **File not scanned** - when a file could not be scanned.

Note

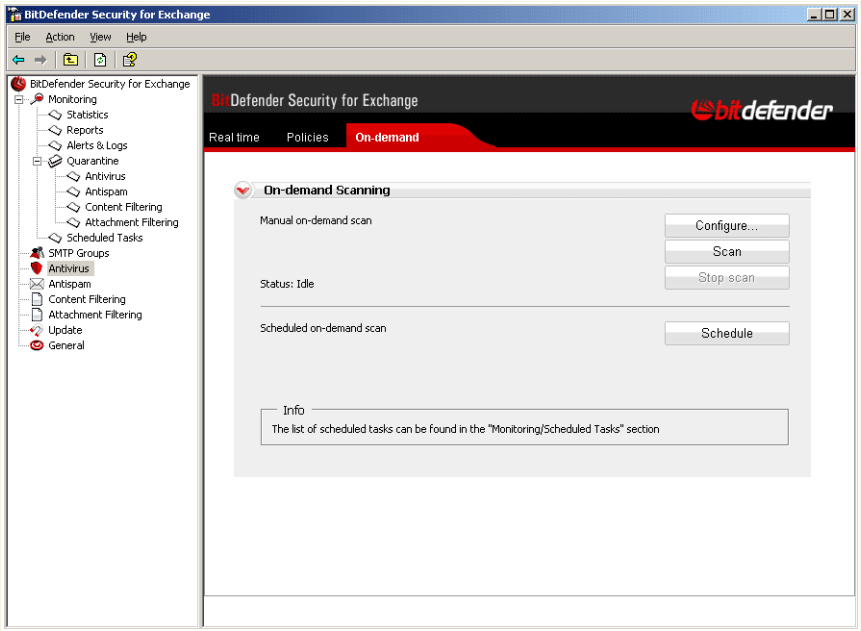
The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Click **OK** to save the changes and close the configuration window.

11.3. On-demand Scanning

BitDefender can scan the Exchange databases (mailboxes and public folders) for viruses and spyware on-demand. To configure and initiate on-demand scanning processes, click **Antivirus** in the tree menu and then the **On-demand** tab.

Note
On-demand scanning is available only for back-end Exchange servers.



On-demand Scanning

In order to perform an on-demand scan, you must configure the scan settings and then click **Scan**. You can stop the scan process anytime you want by clicking **Cancel**.

Note

Only one on-demand scan can be run at a time. Please note that on-demand scanning increases resource consumption. You should not set BitDefender to scan the Exchange databases when the server workload is at a high level.

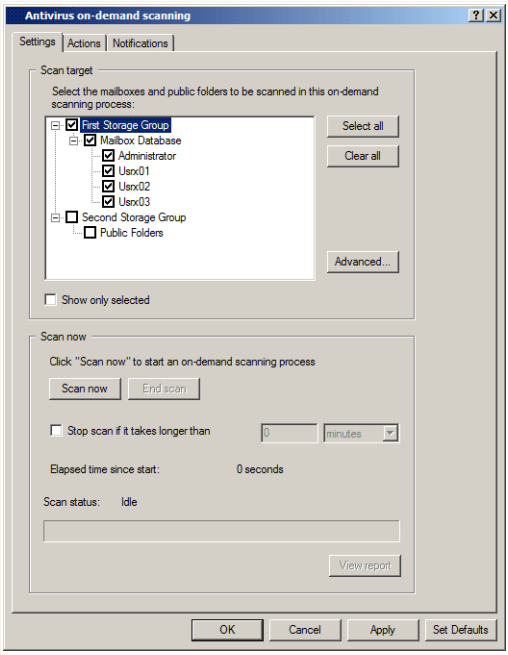
If you want to schedule an on-demand scan, click **Schedule** and follow the steps of the wizard. For more information, please refer to "*On-demand Scanning Tasks*" (p. 103).

11.3.1. Configuring Scan Settings

Click **Configure** to open the window where you can configure the settings of the on-demand scan. Follow these steps to configure the scan settings:

Step 1/3 - Configure Scan Settings

Specify the scan target and other scan settings.



On-demand Scan Settings

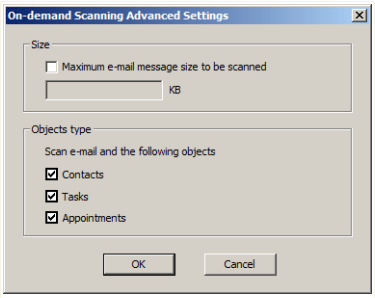
Select Scan Target

Select the check boxes corresponding to the items (groups, mailboxes and public folders) you want to be scanned. If you want to scan all the Exchange databases (mailboxes and public folders), just click **Select All**.

To clear all check boxes and start a new selection, click **Clear All**. You can select **Show only selected** to display only the items to be scanned.

Set Advanced Settings

To set advanced scan settings click **Advanced**. A new window will appear.



Advanced Scan Settings

If you do not want to scan messages that exceed a certain size limit, select **Maximum e-mail message size to be scanned** and provide the size limit in the corresponding field.

Beside messages, you can select other objects to be scanned: **Contacts**, **Tasks** and **Appointments**.

Click **OK** to save changes and close the window.

Scanning

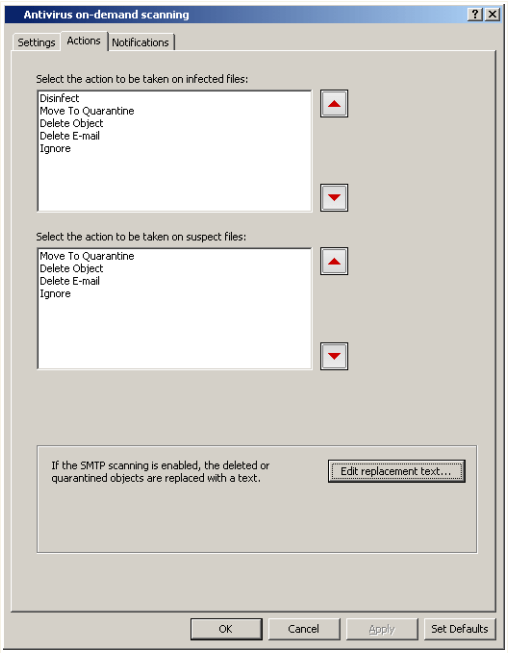
To start scanning, just click **Scan Now**. You can stop the scan process anytime you want to by clicking **End Scan**.

If you want to limit the scanning time, select **Stop scan if it takes longer than** and specify the number of minutes or hours.

At the end of the scanning process, you can return to this section and click **View Report** to view the report file.

Step 2/3 - Set Actions

Click the **Actions** tab and specify the actions to be taken on infected and suspect objects.



Actions

Different actions can be configured for the infected and suspect objects detected by BitDefender. There is a list of actions that can be applied to each category of detected objects (infected or suspect). When such an object is detected, the first action in the corresponding list is applied. If this action fails, the next action in the list is applied and so on.

You can change the order in which actions are to be applied. Select an action and click or to move it up or down in the list.

Actions for infected objects. The following actions are available for infected objects:

Action	*Description*
Disinfect	The infected message is disinfected.

Action	Description
Move to Quarantine	The infected object (mail body / attachment / public file) is moved to the quarantine folder.
Delete object	The infected object (mail body / attachment / public file) is deleted.
Delete e-mail	The infected message is deleted.
Ignore	The infected message is delivered in full to its recipients.

Actions for suspect objects. The following actions are available for suspect objects:

Action	Description
Move to Quarantine	The suspect object (mail body / attachment / public file) is moved to the quarantine folder.
Delete object	The suspect object (mail body / attachment / public file) is deleted.
Delete e-mail	The suspect message is deleted.
Ignore	The suspect message is delivered in full to its recipients.

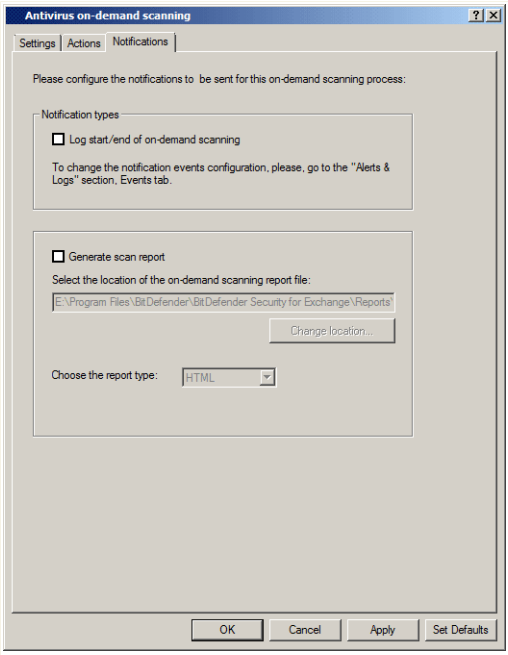
BitDefender replaces the objects that are deleted or moved to quarantine with an explanatory text.

To change the text to be delivered instead of such objects, follow these steps:

1. Click **Edit replacement text...**. A new window will appear.
2. Do any or both of the following:
   - Select **Infected file replaced** and type in the edit box the text to be delivered instead of the infected or suspect objects deleted.
   - Select **Infected file quarantined** and type in the edit box the text to be delivered instead of the infected or suspect objects moved to quarantine.
3. Click **OK** to save the changes and close the window.

Step 3/3 - Configure Notifications

Click the **Notifications** tab and configure the notifications issued for the on-demand scan.



Notifications

Log Scanning

Select **Log start/end of on-demand scanning** to record the start and the end of the on-demand scanning in the log file.

Note

The corresponding event from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Configure Report Settings

Select **Generate scan report** to generate a report for the on-demand scan. By default, the report file is saved in: `C:\Program Files\BitDefender\BitDefender Security for Exchange\Reports`. To change this location click **Change location**.

The report can be generated in HTML, text or CSV format. You can choose the format of the report file from the menu.

Click **OK** to save the changes and close the configuration window.

11.3.2. Viewing Scan Reports

By default, everytime you scan the Exchange server on-demand, a scan report is created. The report provides you with detailed information about the scanning process and the infected files detected.

To view the report of an on-demand scan, go to Reports and double click that report (or select it and click **View Report**). If you are interrested only in the last on-demand scan report, you can open the on-demand scan configuration window, the Settings tab, and click **View Report**.

The report file is displayed using the default browser.

12. Antispam

The Antispam module offers protection against spam, phishing and other attacks. It uses a combination of various filters and engines to determine whether messages are spam or not and to check them for patterns of spam.

Based on the groups the sender and the recipients belong to, you can specify various actions to be taken on the spam messages.

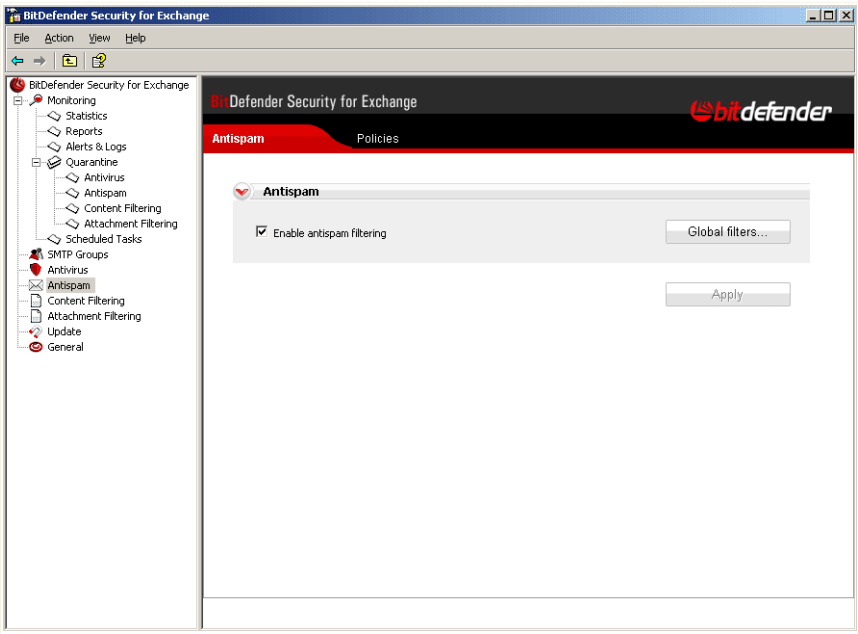
The module contains two sections:

- Antispam Filtering - allows you to enable the antispam filtering and to configure the global antispam filters.
- Policies - allows you to configure the filtering options for all incoming mail traffic and to specify different filtering policies based on the groups the sender and the recipients belong to.

You must configure the global antispam filters in the Antispam tab. Then, go to the Policies and configure the default rule, which controls the antispam policy filters. You can add new rules to create different filtering policies based on the groups the sender and the recipients belong to.

12.1. Antispam Filtering

Click **Antispam** in the tree menu and then the Antispam tab to enter this section.



Antispam Filtering

This is where you can enable antispam filtering and configure the global antispam filters.

If you want the antispam protection to be enabled, select **Enable antispam filtering**. Otherwise, clear this check box.

Click **Apply** to save the changes.

Note

In order to configure the antispam filtering options for all incoming mail traffic or to create different filtering policies based on user groups, go to the Policies section.

12.1.1. Configuring Global Antispam Filters

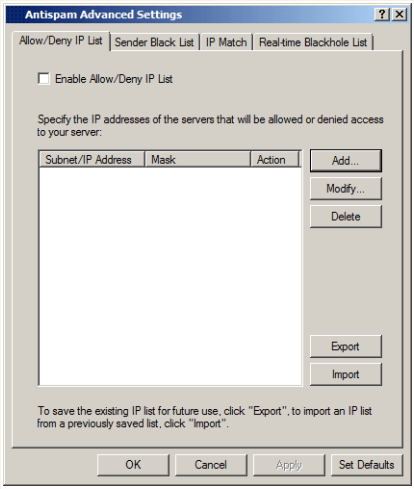
Several global antispam filters can be configured to filter all of the incoming mail traffic, in order to reduce the traffic on the server. These filters are used before a specific group filtering policy is applied.

Note
We recommend you to configure these filters when BitDefender Security for Exchange is installed on a gateway.

Click **Global Filters** to open the configuration window and follow these steps to configure the global antispam filters:

Step 1/4 - Configure Allow / Deny IP List

Click the **Allow / Deny IP List** tab to configure the Allow / Deny IP List.



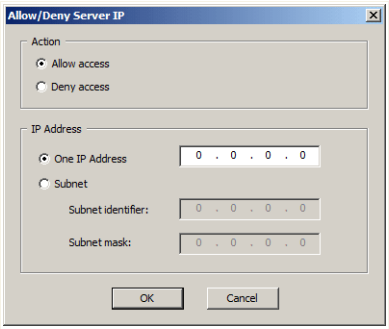
Allow / Deny IP List

The Allow / Deny IP List enables the administrator to specify IP addresses which are denied access to the server. All incoming connections from addresses that appear on the Deny IP List are dropped, provided that such addresses do not appear on the Allow IP List.

Note
The Allow IP List is used to except IP addresses from ranges of IP addresses defined on the Deny IP List.

Select **Enable Allow / Deny IP List** and configure the IP addresses if you want to use the Allow / Deny IP List to filter the incoming mail traffic.

Add IP Addresses. Click **Add** to add a new IP address to the list. The configuration window will appear.



Add IP Address

Follow these steps to configure a new entry on the IP list:

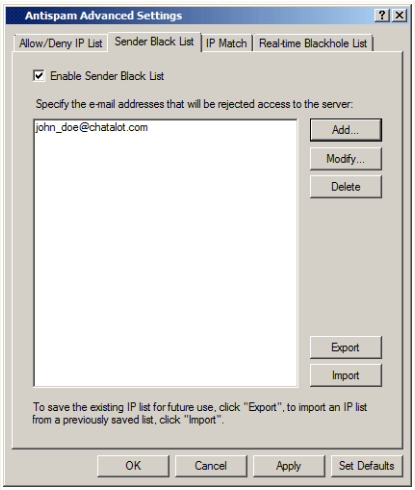
1. Choose the action to be applied to the mail traffic coming from the specified IP address: **Allow access** or **Deny access**.
   - If you select **Deny access**, the incoming connection from the specified IP addresses will be dropped.
   - If you select **Allow access**, messages coming from the specified IP addresses will be allowed to pass.
2. Provide the IP addresses to which the action will apply.
   - If you want to enter a single IP address, select **One IP address** and provide it in the corresponding field.
   - If you want to enter a range of IP addresses, select **Subnet** and provide the subnet identifier and the subnet mask in the corresponding fields.
3. Click **OK** to add the entry to the IP list.

Manage IP List. You can see the IP addresses and the associated action listed in the table. If you want to modify an entry, either double-click it or select it and click **Modify**. To remove one or several selected entries, click **Remove** and then **Yes** to confirm your choice.

Import / Export IP List. To export the IP list to a `txt` file, click **Export** and save the file to the desired location. To import a previously saved list, click **Import**.

Step 2/4 - Configure Sender Black List

Click the **Sender Black List** tab to configure the Sender Black List filter.



Sender Black List

The Sender Black List allows the administrator to specify a list of e-mail addresses which are denied access to the server. The incoming mail from these addresses will be dropped before reaching the server.

Select **Enable Sender Black List** and add the banned addresses if you want to use the Sender Black List to filter incoming mail traffic.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

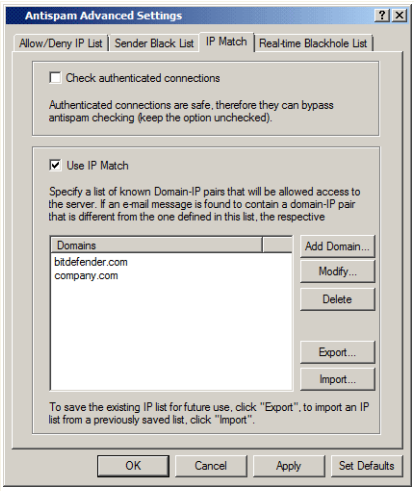
Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. In this way you can use the address list when configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Step 3/4 - Configure IP Match

Click the **IP Match** tab to configure the IP Match filter.


Antispam Advanced Settings
Allow/Deny IP List
Sender Black List
IP Match
Real-time Blackhole List
Check authenticated connections
Authenticated connections are safe, therefore they can bypass antispam checking (keep the option unchecked).
Use IP Match
Specify a list of known Domain-IP pairs that will be allowed access to the server. If an e-mail message is found to contain a domain-IP pair that is different from the one defined in this list, the respective
Domains
bitdefender.com
company.com
Add Domain...
Modify...
Delete
Export...
Import...
To save the existing IP list for future use, click "Export", to import an IP list from a previously saved list, click "Import".
OK
Cancel
Apply
Set Defaults

IP Match

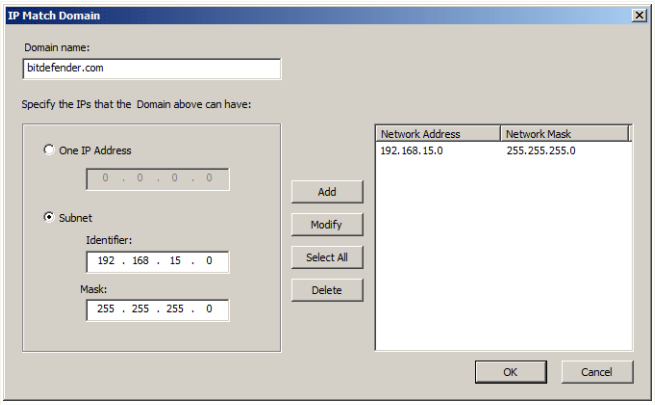
Microsoft Exchange Server 2003 allows authenticating connections. Connections that are authenticated are trusted, therefore they should be allowed to bypass spam detection. However, you can set BitDefender to scan the incoming mail traffic from authenticated sources by selecting **Check authenticated connections**.

Spammers often try to "spoof" the sender's e-mail address to make the e-mail appear as being sent by someone in your domain. To prevent this, you can use IP Match.

If an e-mail appears to be from a domain that you have specified in the IP Match rule list (such as your own company domain), BitDefender checks to see if the IP address of the sender matches the IP addresses provided for the specified domain. If the domain address of the sender matches the IP address, the message bypasses antispam filtering. Otherwise, the connection is dropped.

Select **Use IP Match** and configure the rule list if you want to filter incoming mail traffic using IP Match.

Add Rules. Click **Add** to add a new rule to the list. The configuration window will appear.



Adding Rules

Follow these steps to configure a rule:

1. Provide the domain name in the corresponding field.
2. Provide the IP addresses associated with the specified domain.
   - If you want to enter a single IP address, select **One IP address** and provide it in the corresponding field. Click **Add** to add the entry to the list.
   - If you want to enter a range of IP addresses, select **Subnet** and provide the subnet identifier and the subnet mask in the corresponding fields. Click **Add** to add the entry to the list.

In the table on the right, you can see the IP addresses as they are added. If you want to modify an existing entry, select it, make the necessary changes and click **Modify**.

To select all entries, just click **Select All**. To delete one or several entries from the list, select them and click **Remove** and then **Yes** to confirm your choice.

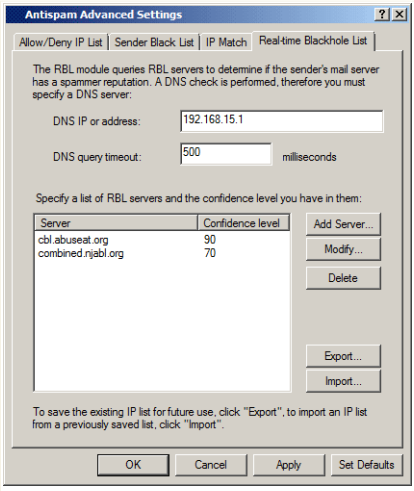
3. Click **OK** to add the rule to the list.

Manage Rules. You can see the existing rules listed in the table. If you want to modify a rule, either double-click it or select it and click **Modify**. To remove one or several selected rules, click **Remove** and then **Yes** to confirm your choice.

Import / Export Rule List. To export the rule list to a `txt` file, click **Export** and save the file to a desired location. To import a previously saved list, click **Import**.

Step 4/4 - Configure Real-time Blackhole List

Click the **Real-time Blackhole List** to configure this filter.



Real-time Blackhole List

The Real-time Blackhole List (RBL) filter allows checking the mail server from which a message is sent against the RBL servers configured by the administrator. It uses

the DNSBL protocol and RBL servers to filter spam based on mail servers' reputation as spam senders.

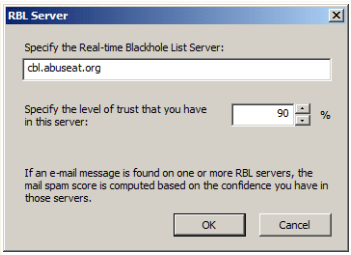
A DNS check is performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com` is the RBL server. If the DNS replies that the domain is valid, it means that the IP is listed in the RBL server and a certain server score is provided. This score ranges between 0 and 100, according to the configured server confidence (trust level).

The query is performed for every RBL server in the list and the score returned by each one is added to the intermediate score. When the score has reached `100`, no more queries are performed.

If the RBL filter score is 100 or higher, the message is considered SPAM and the specified action is taken. Otherwise, a spam score is computed from the RBL filter score and added to the global spam score of the message.

Provide the IP or the address of the DNS server to query and the query timeout interval in the corresponding fields.

Add RBL Servers. Click **Add** to add a new RBL server to the list. The configuration window will appear.


RBL Server
Specify the Real-time Blackhole List Server:
cbl.abuseat.org
Specify the level of trust that you have in this server:
90
%
If an e-mail message is found on one or more RBL servers, the mail spam score is computed based on the confidence you have in those servers.
OK
Cancel

Add RBL Servers

First, specify the name of the RBL server and then the level of trust. The level of trust is an indicator on a scale from 0 to 100 which shows the accuracy you consider the RBL server to have. The value you provide is used when computing the SPAM score. Click **OK** to add the RBL server to the list.

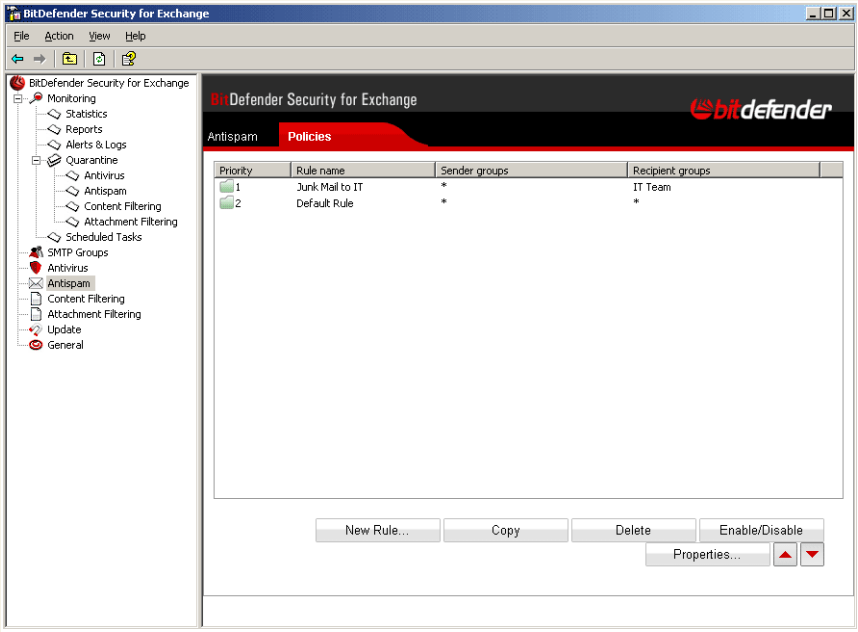
Manage RBL Servers. You can see the RBL servers listed in the table. If you want to modify the settings for an RBL server, either double-click it or select it and click **Modify**. To remove one or several selected RBL servers, click **Remove** and then **Yes** to confirm your choice.

Import / Export RBL Servers. To export the existing RBL servers and their settings to a `txt` file, click **Export** and save the file to the desired location. To import a previously saved database of RBL servers click **Import**.

Click **OK** to save the changes and close the configuration window.

12.2. Policies

Click **Antispam** in the tree menu and then the **Policies** tab to enter this section.



Policies

This is where you can specify the antispam filtering options. You can modify the default rule to specify the antispam filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

12.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and recipients it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note

Messages are checked against each rule, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the antispam filtering options specified by that rule.

Please note that the mail traffic is first filtered using the global antispam filters. The messages that pass the global filters are then checked against the existing policies. For more information, please refer to "*Configuring Global Antispam Filters*" (p. 152).

Default Rule. There is one rule created by default that manages the antispam filtering settings for all groups. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. In this way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables / disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 161).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

12.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.

- click **New Rule** and configure the new rule.

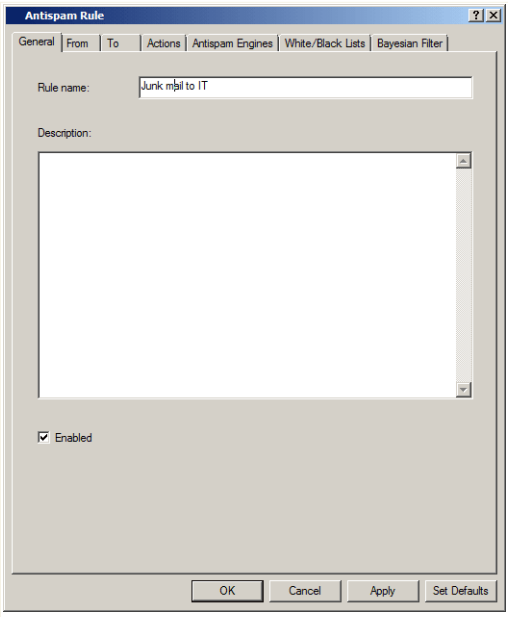
In both cases, a new window will appear. Next, you must configure or modify the rule.

12.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/7 - Provide General Data

Open the configuration window and provide general data for the rule.



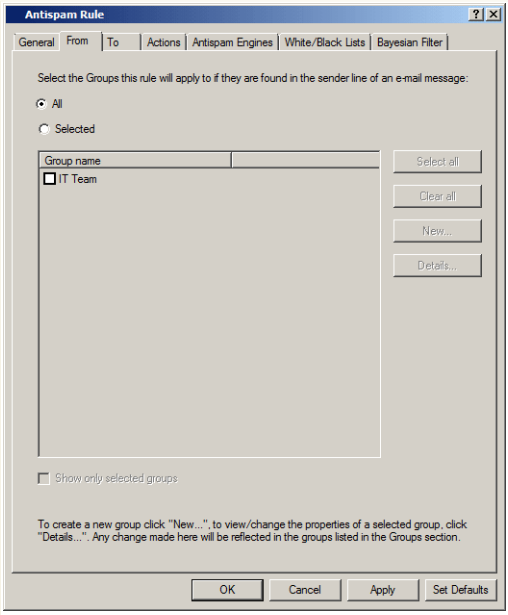
General

Provide the rule name and, optionally, the rule description.

To enable the rule, select **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/7 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to senders from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

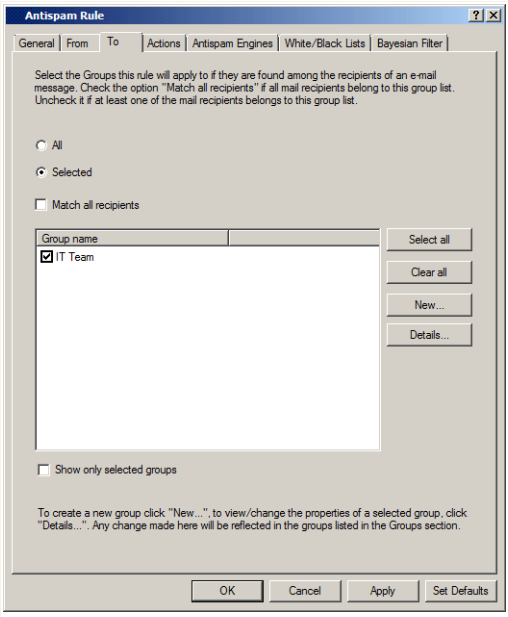
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 3/7 - Select Recipients Groups

Click the **To** tab and select the groups of recipients the rule applies to.


Antispam Rule
General
From
To
Actions
Antispam Engines
White/Black Lists
Bayesian Filter
Select the Groups this rule will apply to if they are found among the recipients of an e-mail message. Check the option "Match all recipients" if all mail recipients belong to this group list. Uncheck it if at least one of the mail recipients belongs to this group list.
All
Selected
Match all recipients
Group name
IT Team
Select all
Clear all
New...
Details...
Show only selected groups
To create a new group click "New...", to view/change the properties of a selected group, click "Details...". Any change made here will be reflected in the groups listed in the Groups section.
OK
Cancel
Apply
Set Defaults

Recipients Groups

The following options are available:

- **All** - the rule applies to all recipients, no matter if they belong to a group or not.
- **Selected** - the rule applies only to recipients from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all recipients** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several

recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note
The addresses in the **Cc** and **Bcc** fields also count as recipients.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

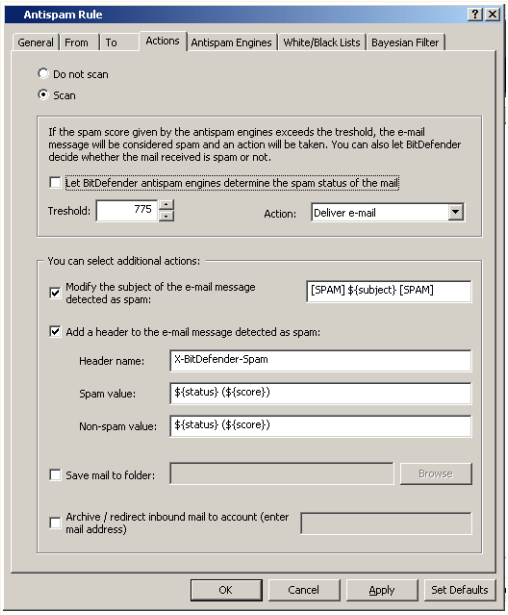
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 4/7 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the messages matching this policy.



Actions

If you do not want the messages to be scanned using the antispam filters, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the antispam filters and the antispam options configured for this policy. Next, you must configure the threshold level and the actions to be taken on the spam messages.

Specify Threshold Level

BitDefender checks all the message components (i.e. not only the header but also the message body in either HTML or text format) against many rules, using several filters. Some of the filters, like the URL Filter, the Image Filter and others, can indicate if the message is spam directly.

The Bayesian Filter, the Pre-trained Bayesian Filter and the NeuNet Filter give to each scanned message a Spam score. The aggregate of these scores represents an overall spam score.

The overall spam score is measured against the desired level of spam sensitivity (threshold), and a decision is made. If the spam score for a message exceeds the threshold, the message is considered spam. Otherwise, the message is not spam and it is delivered in full to its recipients.

Note
Exceptions are made if the sender is in the IPMatch table (as not spam) or on the White list.

Specify a threshold value between 0 and 1000 in the corresponding field. The default value is 775.

If you do not want to set a threshold value, select **Let BitDefender antispam engines determine the spam status of the mail** to let the BitDefender Antispam Engine to decide whether a message is spam or not.

Set Actions

Choose from the menu one of the following actions to be taken on the spam messages:

Action	Description
Deliver e-mail	The spam message is delivered in full to its recipients.
Delete e-mail	The spam message is deleted.
Quarantine	The spam message is moved to the quarantine folder.
Reject e-mail	The spam message is rejected with a 550 SMTP error code.

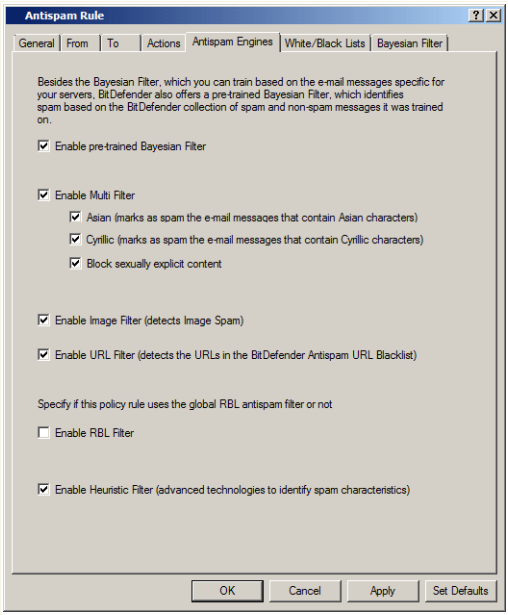
In order to help you process spam messages, several additional actions are available:

Action	Description
Modify the subject of the e-mail message detected as spam	The subject of the messages detected as spam is modified. You can modify the subject pattern. We recommend you to use one of these patterns:

Action	Description
	• `[SPAM]${subject}[SPAM]` - to add `[SPAM]` before and after the subject. This is the default subject pattern. • `[SPAM]` - to replace the subject with `[SPAM]`. • `[$score% SPAM]$subject` - to add `[x SPAM]` before the subject, where `x` represents the spam score.
Add a header to the e-mail message detected as spam	An e-mail header is added to the messages detected as spam. You can modify the header name and the spam and non-spam values. By default, the spam and non-spam values are `${status} (${score})`. This means that for a spam message the header will be `Name: Yes(x)`, while for a legitimate message the header will be `Name: No(x)`, where `x` represents the spam score received by the message.
Save e-mail to folder	The spam message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive / redirect to account	The spam message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 5/7 - Configure Antispam Engines

Click the **Antispam Engines** tab and specify which antispam engines to be enabled.


Antispam Rule
General
From
To
Actions
Antispam Engines
White/Black Lists
Bayesian Filter
Besides the Bayesian Filter, which you can train based on the e-mail messages specific for your servers, BitDefender also offers a pre-trained Bayesian Filter, which identifies spam based on the BitDefender collection of spam and non-spam messages it was trained on.
Enable pre-trained Bayesian Filter
Enable Multi Filter
Asian (marks as spam the e-mail messages that contain Asian characters)
Cyrillic (marks as spam the e-mail messages that contain Cyrillic characters)
Block sexually explicit content
Enable Image Filter (detects Image Spam)
Enable URL Filter (detects the URLs in the BitDefender Antispam URL Blacklist)
Specify if this policy rule uses the global RBL antispam filter or not
Enable RBL Filter
Enable Heuristic Filter (advanced technologies to identify spam characteristics)
OK
Cancel
Apply
Set Defaults

Antispam Engines

Note

For more information on the antispam filters mentioned here, please refer to "*Policy Filters*" (p. 18).

The following options are available:

- **Enable pre-trained Bayesian Filter** - enables / disables the pre-trained Bayesian Filter.
- **Enable Multi Filter** - enables / disables the Multi Filter.

  This filter has several components:

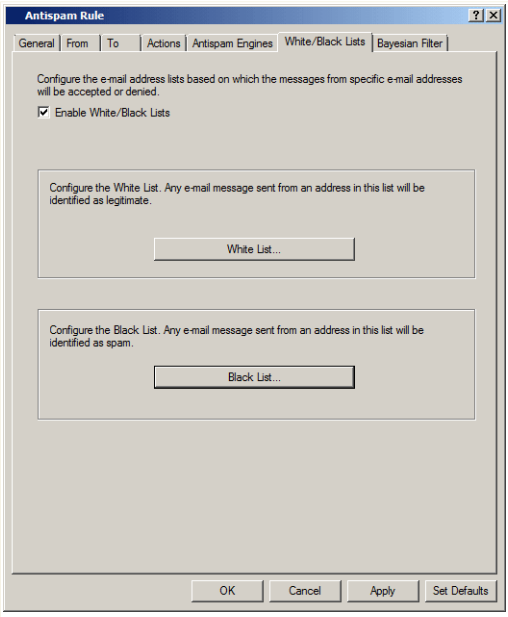
  - **Asian** - enables / disables the filter that blocks mail written in Asian characters.
  - **Cyrillic** - enables / disables the filter that blocks mail written in Cyrillic characters.
  - **Block sexually explicit content** - enables / disables the filter that blocks messages tagged `Sexually-Explicit` in the subject.

- **Enable Image Filter** - enables / disables the Image Filter.
- **Enable URL Filter** - enables / disables the URL Filter.
- **Enable RBL Filter** - enables / disables the global RBL Filter.
- **Enable Heuristic Filter** - enables / disables the Heuristic Filter.

Note
To enable / disable a filter select / clear the corresponding check box.

Step 6/7 - Configure White List / Black List

Click the **White / Black Lists** tab and configure the White List and the Black List.


Antispam Rule
General
From
To
Actions
Antispam Engines
White/Black Lists
Bayesian Filter
Configure the e-mail address lists based on which the messages from specific e-mail addresses will be accepted or denied.
Enable White/Black Lists
Configure the White List. Any e-mail message sent from an address in this list will be identified as legitimate.
White List...
Configure the Black List. Any e-mail message sent from an address in this list will be identified as spam.
Black List...
OK
Cancel
Apply
Set Defaults

White List / Black List

Most people communicate regularly with a group of people or even receive messages from companies or organizations in the same domain. By using the White List / Black

List filter, the administrator can set a list of trusted and untrusted addresses from which to respectively "always accept" or "always reject" e-mail messages.

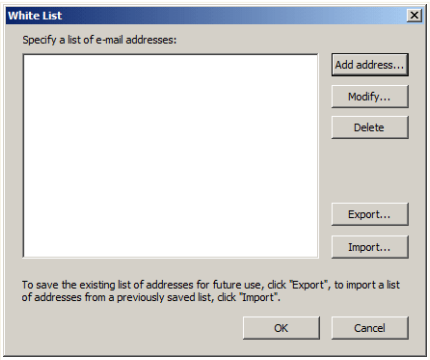
Select **Enable White / Black Lists** to filter messages using the White List and the Black List.

White List

The White List contains e-mail addresses expected to send legitimate messages. Any mail coming from an address contained in the **White list** will be considered legitimate and will bypass further antispam filters.

Note
We recommend that you add the trusted addresses to the White List. BitDefender does not block messages coming from the addresses on the list; therefore, adding them helps ensure that legitimate messages get through.

Click **White List** to configure the White List. A new window will appear.


White List
Specify a list of e-mail addresses:
Add address...
Modify...
Delete
Export...
Import...
To save the existing list of addresses for future use, click "Export", to import a list of addresses from a previously saved list, click "Import".
OK
Cancel

White List

This is where you can see and manage trusted e-mail addresses.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

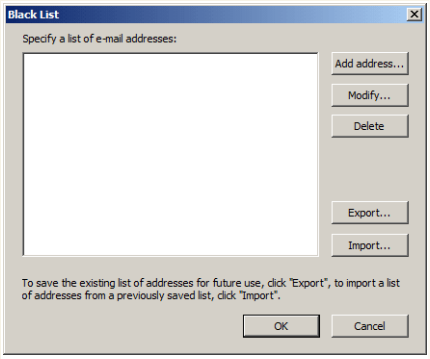
Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. In this way you can use the address list when configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Black List

The Black List contains e-mail addresses expected to send spam messages. Any mail coming from an address contained in the **Black list** will be considered spam and the appropriate action will be taken.

Click **Black List** to configure the Black List. A new window will appear.


Black List
Specify a list of e-mail addresses:
Add address...
Modify...
Delete
Export...
Import...
To save the existing list of addresses for future use, click "Export", to import a list of addresses from a previously saved list, click "Import".
OK
Cancel

Black List

This is where you can see and manage untrusted e-mail addresses.

Add Addresses. Click **Add** to add a new address to the list. Provide the address in the window that will appear and then click **OK**.

Manage Addresses. You can see the e-mail addresses listed in the table. If you want to modify an address, either double-click it or select it and click **Modify**. To remove one or several selected addresses, click **Delete** and then **Yes** to confirm your choice.

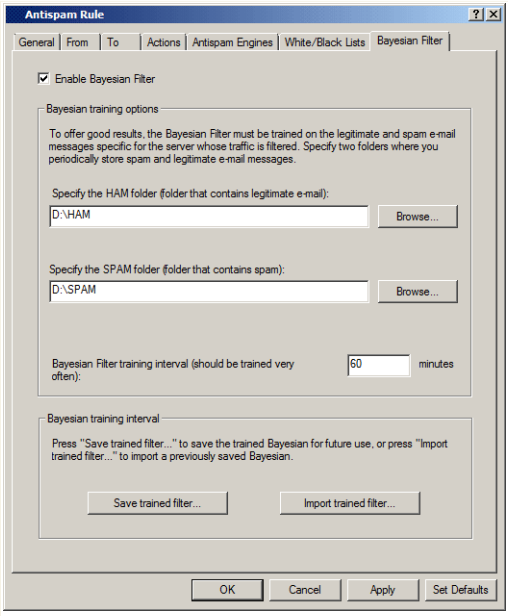
Import / Export Addresses. To import addresses from a `txt` file, click **Import**, select it and then click **Open**. To export the existing addresses to a `txt` file, click **Export** and save the file to the desired location. In this way you can use the address list when

configuring BitDefender server products on other machines or after reinstalling the product.

Click **OK** to save the changes and close the window. If you click **Cancel** all changes will be lost.

Step 7/7 - Configure Bayesian Filter

Click the **Bayesian Filter** tab and configure the Bayesian Filter.


Antispam Rule
General
From
To
Actions
Antispam Engines
White/Black Lists
Bayesian Filter
Enable Bayesian Filter
Bayesian training options
To offer good results, the Bayesian Filter must be trained on the legitimate and spam e-mail messages specific for the server whose traffic is filtered. Specify two folders where you periodically store spam and legitimate e-mail messages.
Specify the HAM folder (folder that contains legitimate e-mail):
D:\HAM
Browse...
Specify the SPAM folder (folder that contains spam):
D:\SPAM
Browse...
Bayesian Filter training interval (should be trained very often):
60
minutes
Bayesian training interval
Press "Save trained filter..." to save the trained Bayesian for future use, or press "Import trained filter..." to import a previously saved Bayesian.
Save trained filter...
Import trained filter...
OK
Cancel
Apply
Set Defaults

Bayesian Filter

The Bayesian Filter constantly collects statistical information about server-specific spam and legitimate messages provided by the administrator and it analyzes messages according to this information.

Select **Enable Bayesian Filter** to enable the Bayesian Filter.

To offer good results, the Bayesian Filter must be trained on legitimate messages and spam messages specific to the server whose traffic is filtered. These messages must be in MIME format; this means that they should have the `.eml` extension. Specify the

HAM folder (the folder containing legitimate mail) and the **SPAM folder** by clicking **Browse**.

Note
The messages in the SPAM and HAM folders are deleted after the training is completed.

In order to get the best results, it is recommended to train the Bayesian Filter often. Provide the training interval in the corresponding field. The recommended interval is 60 minutes.

Warning
Do not set very low values for the training interval, otherwise the Bayesian Filter will not have enough time to complete one training before another one starts. This means that instead of analyzing messages, it will only train itself continuosly.

To save the current Bayesian dictionary for future use, click **Save trained filter**. If you have a Bayesian dictionary that was previously saved with the **Save trained filter** option, you can import it by clicking **Import trained filter**.

Click **OK** to save the changes and close the configuration window.

13. Content Filtering

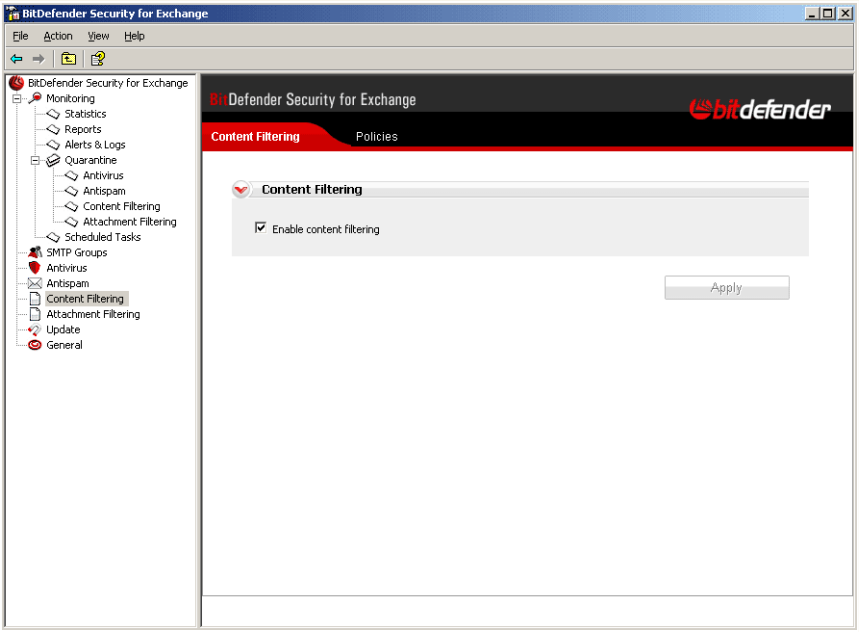
Content Filtering helps you filter e-mail messages based on certain character strings found in the e-mail headers (subject, from, to, cc) or in the e-mail body. By using Content Filtering, you can achieve the following goals:

- prevent unwanted mail content from entering the Exchange server mailboxes.
- block outgoing mail containing confidential data.
- archive messages that meet specific conditions (for example, those coming on your company's support e-mail address) to a different e-mail account or on the disk.

Content Filtering is by default enabled, but all messages are allowed to pass without being scanned. To use Content Filtering, go to the Policies tab and configure the default rule. The default rule manages the content filtering settings for all mail traffic reaching or leaving the server. By adding new rules, you can create different filtering policies based on the groups the sender and the recipients belong to.

13.1. Content Filtering

Click **Content Filtering** in the tree menu to enter this section.



Content Filtering

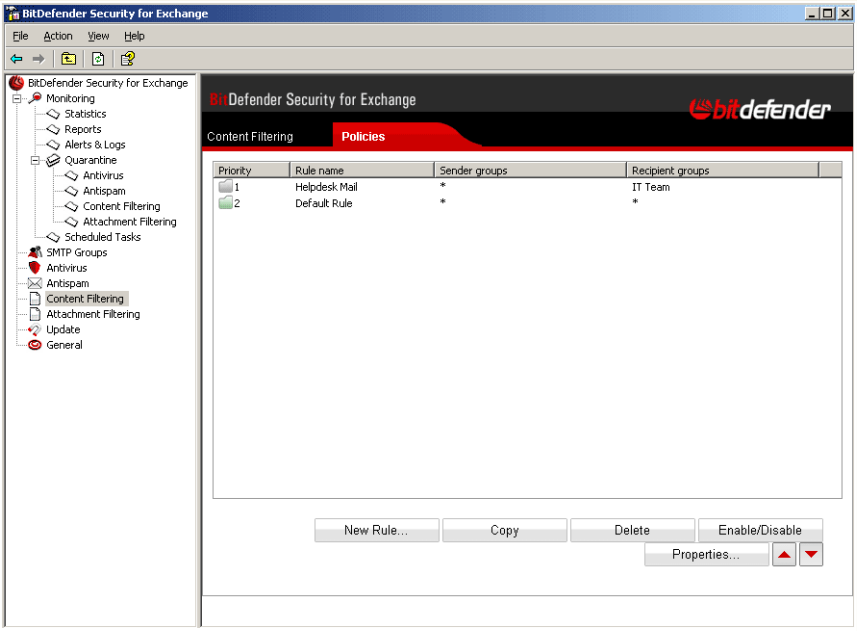
This is where you can enable content filtering.

If you want content filtering to be enabled, select **Enable content filtering**. Otherwise, clear this check box. Click **Apply** to save the changes.

Note
In order to configure the global content filtering options or to create different filtering policies based on user groups, go to the Policies section.

13.2. Policies

Click **Content Filtering** in the tree menu and then the **Policies** tab to enter this section.



Policies

This is where you can specify the content filtering options. You can modify the default rule to specify the content filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

13.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and recipients it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note
Messages are checked against each rule, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the content filtering options specified by that rule.

Default Rule. There is one rule created by default that manages the global content filtering settings. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. In this way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables / disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 178).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

13.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

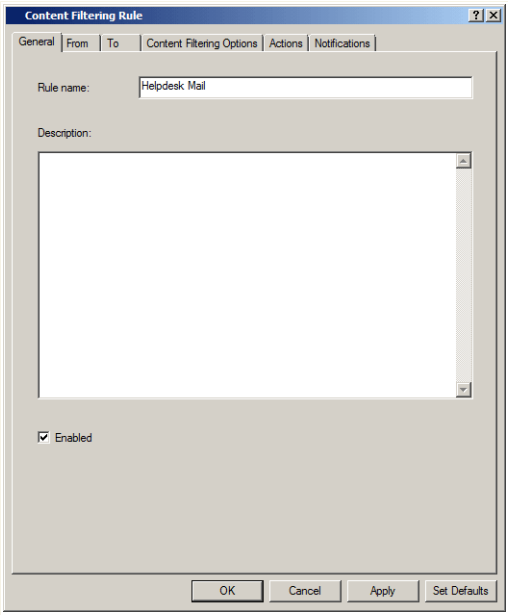
In both cases, a new window will appear. Next, you must configure or modify the rule.

13.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/6 - Provide General Data

Open the configuration window and provide general data for the rule.



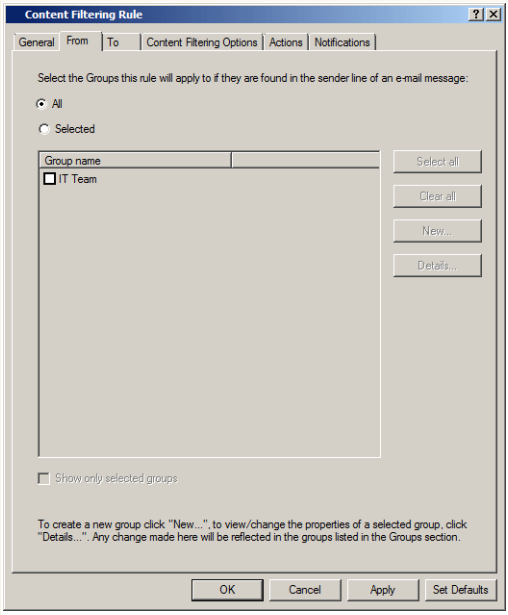
General

Provide the rule name and, optionally, the rule description.

To enable the rule, select **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/6 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to senders from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

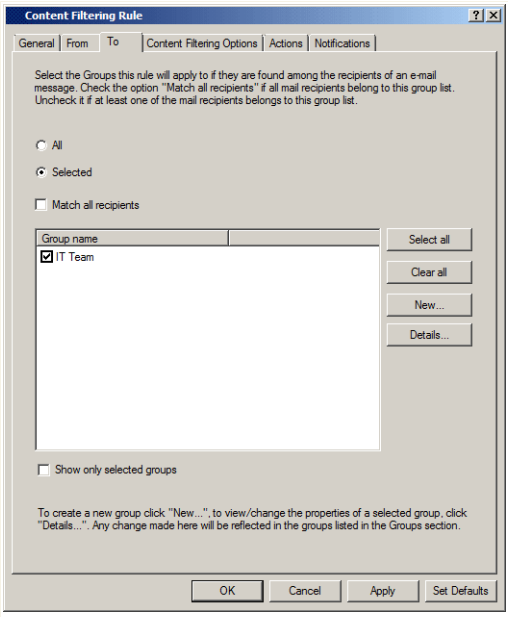
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 3/6 - Select Recipients Groups

Click the **To** tab and select the groups of recipients the rule applies to.


Content Filtering Rule
General
From
To
Content Filtering Options
Actions
Notifications
Select the Groups this rule will apply to if they are found among the recipients of an e-mail message. Check the option "Match all recipients" if all mail recipients belong to this group list. Uncheck it if at least one of the mail recipients belongs to this group list.
All
Selected
Match all recipients
Group name
IT Team
Select all
Clear all
New...
Details...
Show only selected groups
To create a new group click "New...", to view/change the properties of a selected group, click "Details...". Any change made here will be reflected in the groups listed in the Groups section.
OK
Cancel
Apply
Set Defaults

Recipients Groups

The following options are available:

- **All** - the rule applies to all recipients, no matter if they belong to a group or not.
- **Selected** - the rule applies only to recipients from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all recipients** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several

recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note
The addresses in the **Cc** and **Bcc** fields also count as recipients.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

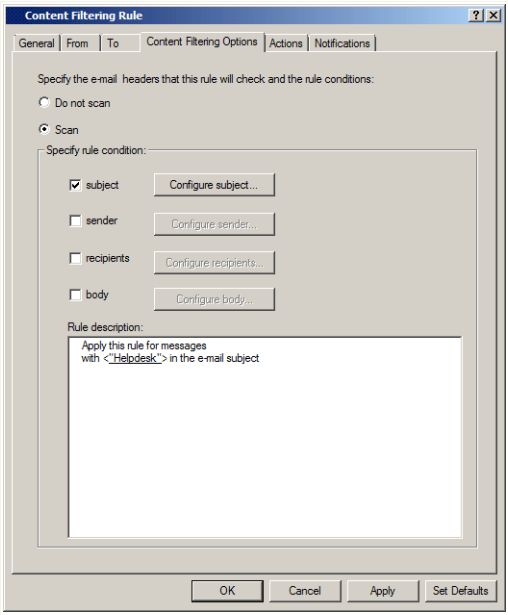
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 4/6 - Configure Content Filtering Options

Click the **Content Filtering Options** tab and configure the content filtering options for the messages matching this policy.



Filtering Options

If you do not want the messages to be scanned using content filtering options, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the content filtering options configured for this policy. Next, you must specify the rule conditions.

Note
Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Messages can be scanned using the following criteria: subject, sender / recipient address, body. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Mail by Subject

Select **Subject** and specify the rule strings in order to filter mail by subject. All the messages the subject of which matched one of the defined strings will be detected.

To specify the strings, click **Configure subject**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 183)).

Filtering Mail by Sender Address

Select **Sender** and specify the rule strings in order to filter mail by the sender address. All the messages the sender address of which matches one of the defined strings will be detected.

To specify the strings, click **Configure sender**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 183)).

Filtering Mail by Recipients Address

Select **Recipients** and specify the rule strings in order to filter mail by the recipient address. All messages with at least one recipient address matching one of the defined strings will be detected.

To specify the strings, click **Configure recipients**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 183)).

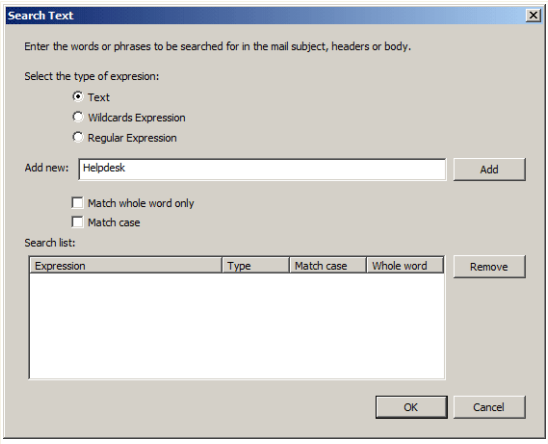
Filtering Mail by Body Content

Select **Body** and specify the rule strings in order to filter mail by content. All messages containing one of the defined strings in the e-mail body will be detected.

To specify the strings, click **Configure body**. A new window will appear, where you can configure the defined strings (please see "*Configuring Strings*" (p. 183)).

Configuring Strings

You can see each selected rule condition listed in the box. Click the `specific words` link to specify or modify strings. A configuration window will appear.



Specify parameters

Provide the string in the corresponding field and click **Add**.

You can choose to enter either a wildcard expression or a regular expression.

Note
You can use the following wildcards:

- `*` replaces zero, one or more characters.

  For example, you can enter `*xxx*` to detect the messages that contain the `xxx` string in the headers (subject, sender address or recipient address).

- `?` stands for any single character.

  For example, if you filter messages by the sender address, you can add `?doe@company.com` to detect the messages that are sent from addresses beginning with any single character and followed by the `doe@company.com` string.

Two additional options are available:

Option	*Description*
Match case	The rule applies only if the detected item and the specified parameter case match.

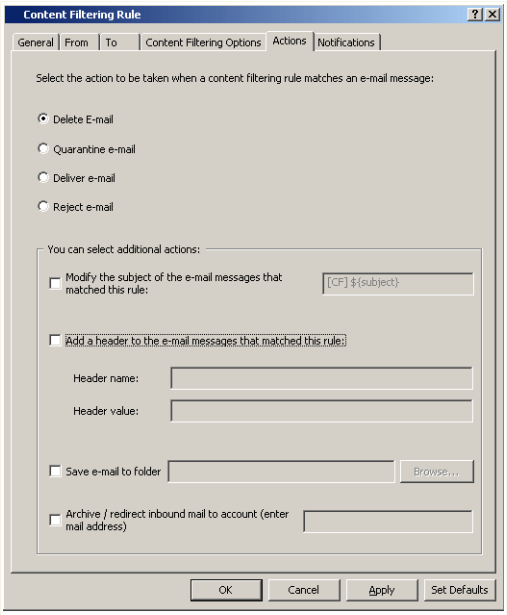
Option	Description
Match whole word only	The rule applies only if an entire string matching the specified parameter is detected.

You can see all the defined strings in the list. To remove entries, select them and click **Remove**.

Click **OK** to save the changes.

Step 5/6 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the detected messages.



Actions

You must choose one of the following actions:

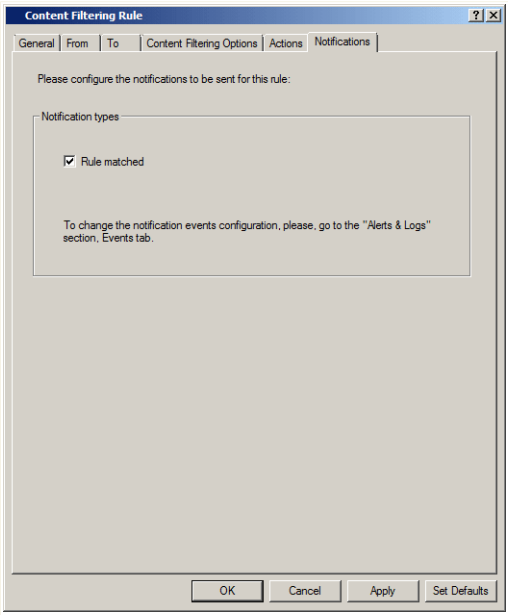
Action	Description
Delete e-mail	The detected message is deleted.
Quarantine e-mail	The detected message is moved to the quarantine folder.
Deliver e-mail	The detected message is delivered in full to its recipients.
Reject e-mail	The detected message is rejected with a 550 SMTP error code.

You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the e-mail messages that matched this rule	The subject of the detected message is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[CF]${subject}` - to add `[CF]` before the subject. This is the default subject pattern. • `[CF]${subject}[CF]` - to add `[CF]` before and after the subject. • `[CF]` - to replace the subject with `[CF]`.
Add a header to the e-mail messages that matched this rule	An e-mail header is added to the detected message. Provide the header name and value in the corresponding fields.
Save e-mail to folder	The detected message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 6/6 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when messages match the rule.



Notifications

Select **Rule matched** to issue notifications when messages match the rule.

Note

The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Click **OK** to save the changes and close the configuration window.

14. Attachment Filtering

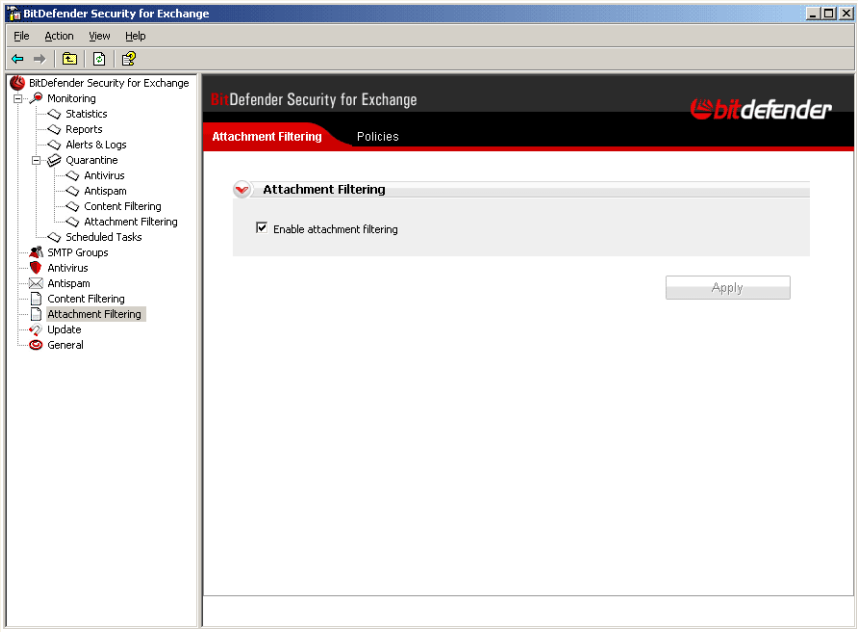
The Attachment Filtering module provides filtering features for mail attachments. It can detect attachments with certain name patterns, of a certain type or exceeding a certain size limit. By using Attachment Filtering, you can achieve the following goals:

- limit the size of the attachments entering or leaving the Exchange server mailboxes.
- block potentially dangerous attachments, such as `.vbs` or `.exe` files, or the e-mails containing them (for example, quarantine e-mail or delete attachment)
- block attachments having offensive names or the e-mails containing them (for example, reject e-mail or delete attachment)

Attachment Filtering is by default enabled, but all messages are allowed to pass without being scanned. To use Attachment Filtering, go to the Policies tab and configure the default rule. The default rule manages the attachment filtering settings for all mail traffic reaching or leaving the server. By adding new rules, you can create different filtering policies based on the groups the sender and the recipients belong to.

14.1. Attachment Filtering

Click **Attachment Filtering** in the tree menu to enter this section.



Attachment Filtering

This is where you can enable attachment filtering.

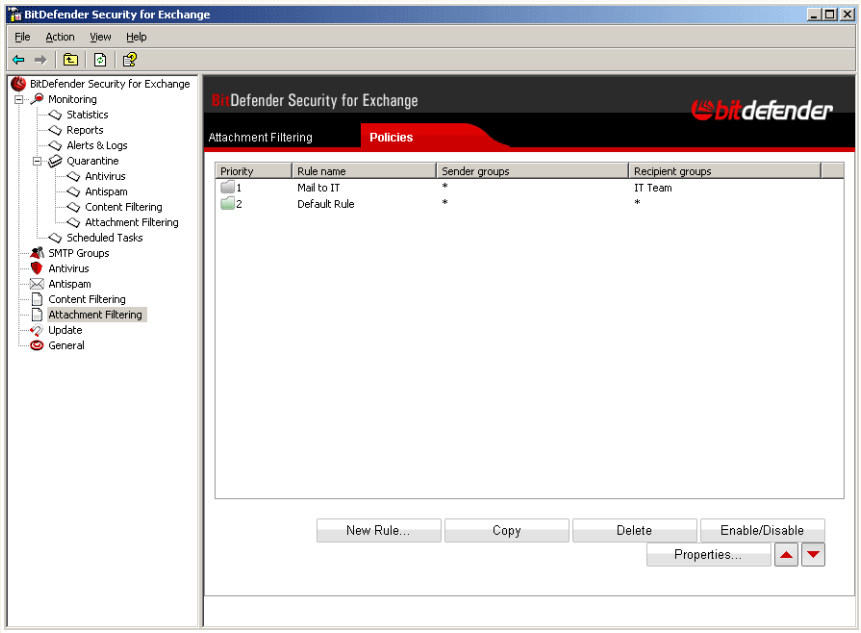
If you want attachment filtering to be enabled, select **Enable attachment filtering**. Otherwise, clear this check box. Click **Apply** to save the changes.

Note

In order to configure the global attachment filtering options or to create different filtering policies based on user groups, go to the Policies section.

14.2. Policies

Click **Attachment Filtering** in the tree menu and then the **Policies** tab to enter this section.



Policies

This is where you can specify the attachment filtering options. You can modify the default rule to specify the attachment filtering options for all of the mail traffic, or you can configure new rules in order to create customized group filtering policies.

14.2.1. Managing Rules

You can see all the existing rules listed in the table. For each rule, the following information is provided: priority, the name and the groups of senders and recipients it applies to. The rules are listed by order of priority with the first rule counting as the highest priority.

Note
Messages are checked against each rule, by order of priority, until the sender and the recipients of the message match a rule. The message is then processed according to the attachment filtering options specified by that rule.

Default Rule. There is one rule created by default that manages the global content filtering settings. You cannot copy, delete or disable this rule. The default rule has the lowest priority; therefore, you cannot change its priority. Because the rule was designed to apply to the entire mail traffic, you cannot configure group options. However, you can configure all the other options.

Group Filtering Policies. To set different filtering policies, add new rules. In this way you can create customized filtering rules for the mail traffic between certain groups of users.

To manage the rules, use the following buttons:

- **New Rule** - creates a new rule. You will have to configure the rule before it appears in the table.
- **Copy** - copies one or several selected rules.
- **Delete** - deletes one or several selected rules. You will have to confirm your choice by clicking **Yes**.
- **Enable / Disable** - enables / disables one or several selected rules.
- **Properties** - opens the configuration window of a selected rule, allowing you to modify the rule. To learn how to configure the rule, please refer to "*Configuring Rules*" (p. 192).
- **Up** - moves a selected rule one level up in the table. This will increase the priority of the rule.
- **Down** - moves a selected rule one level down in the table. This will decrease the priority of the rule.

14.2.2. Creating Rules

To create a rule, choose one of these methods:

- copy an existing rule and click **Properties** to modify it.
- click **New Rule** and configure the new rule.

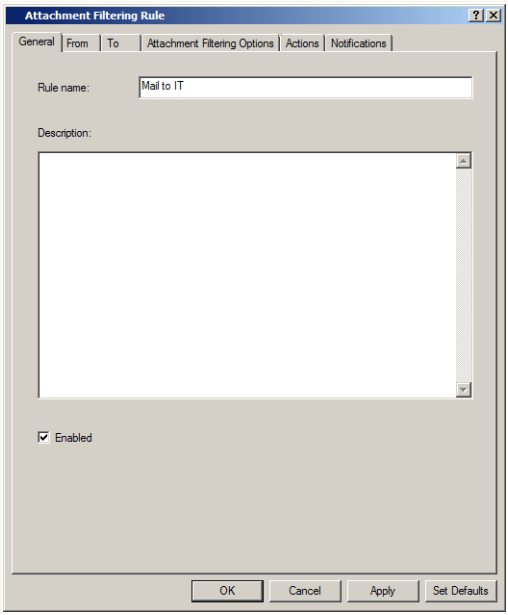
In both cases, a new window will appear. Next, you must configure or modify the rule.

14.2.3. Configuring Rules

To configure a rule follow these steps:

Step 1/6 - Provide General Data

Open the configuration window and provide general data for the rule.



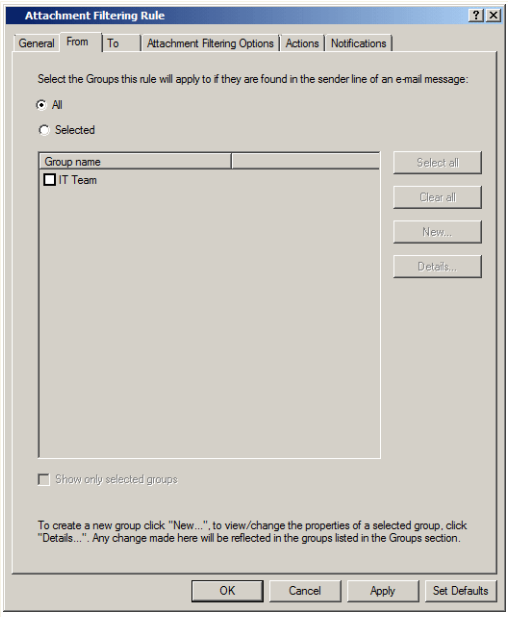
General

Provide the rule name and, optionally, the rule description.

To enable the rule, select **Enabled**. If you want the rule to be disabled, clear the check box.

Step 2/6 - Select Senders Groups

Click the **From** tab and select the groups of senders the rule applies to.



Senders Groups

The following options are available:

- **All** - the rule applies to all senders, no matter if they belong to a group or not.
- **Selected** - the rule applies only to senders from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

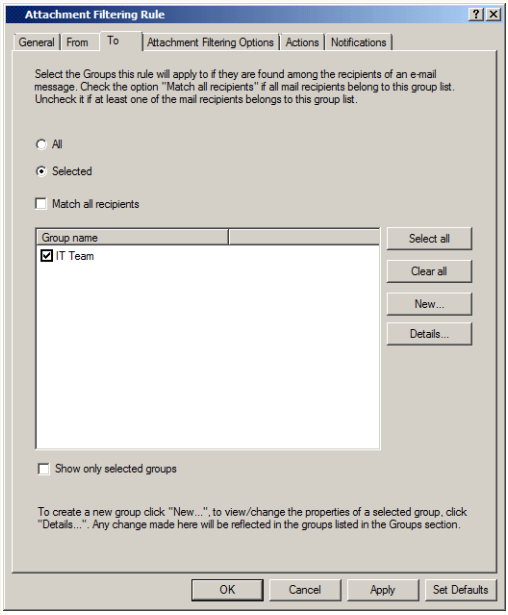
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 3/6 - Select Recipients Groups

Click the **To** tab and select the groups of recipients the rule applies to.


Attachment Filtering Rule
General
From
To
Attachment Filtering Options
Actions
Notifications
Select the Groups this rule will apply to if they are found among the recipients of an e-mail message. Check the option "Match all recipients" if all mail recipients belong to this group list. Uncheck it if at least one of the mail recipients belongs to this group list.
All
Selected
Match all recipients
Group name
IT Team
Select all
Clear all
New...
Details...
Show only selected groups
To create a new group click "New...", to view/change the properties of a selected group, click "Details...". Any change made here will be reflected in the groups listed in the Groups section.
OK
Cancel
Apply
Set Defaults

Recipients Groups

The following options are available:

- **All** - the rule applies to all recipients, no matter if they belong to a group or not.
- **Selected** - the rule applies only to recipients from the selected groups.

If you choose **Selected**, you have to select from the list the groups you want the rule to apply to.

You can select **Match all recipients** to apply the rule only if all the recipients of the message belong to the specified groups. For example, if the e-mail is sent to several recipients and at least one of them is not found in the specified groups, the rule will not apply.

Note
The addresses in the **Cc** and **Bcc** fields also count as recipients.

Click **Select All** to select all groups. If you click **Clear All** no group will be selected.

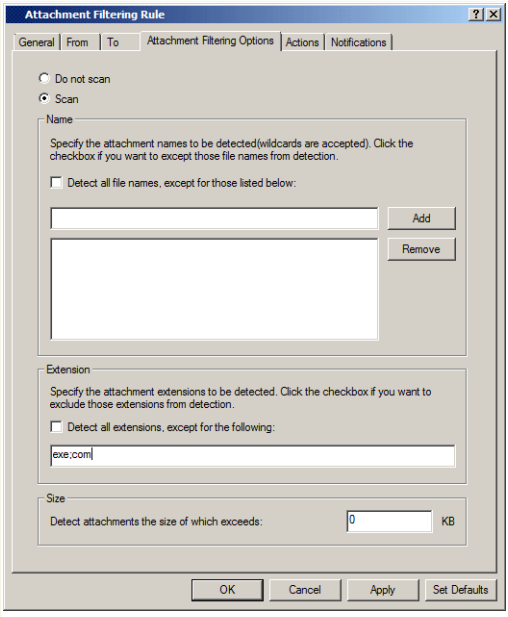
If necessary, you can create a new group by clicking **New** and configuring it. The new group will appear in the Groups section.

To configure an existing group or to see its parameters, select it and click **Details**.

Note
To learn how to configure a group, please refer to "*Creating Groups*" (p. 121).

Step 4/6 - Configure Attachment Filtering Options

Click the **Attachment Filtering Options** tab and configure the filtering options for the messages matching this policy.



Filtering Options

If you do not want the messages to be scanned using attachment filtering options, select **Do not scan**. Then, click **OK** to save the changes and close the configuration window.

If you select **Scan**, the messages will be scanned using the attachment filtering options configured for this policy. Next, you must specify the rule conditions.

Note
Messages that do not match any rule condition will not be detected. Consequently, no action will be taken on them and no notification will be issued.

Mail attachments can be scanned using the following criteria: name, file extension and file size. When defining rule conditions, any combination of scanning criteria is allowed.

Filtering Attachments by Name

Select **Detect all filenames except those listed below** and specify the excepted filenames in order to filter attachments by name. All attachments with filenames other than those specified as exceptions will be detected.

Note
The term `name` refers here to the filename and the filename extension. For example, if the filename is `name_of_file` and the filename extension is `ext`, then the name you have to specify as exception is `name_of_file.ext`.

To specify exceptions, provide the name in the edit field and click **Add**.

Note
Wildcards can be used to specify exceptions:

- `*` replaces zero, one or more characters.

  For example, you can enter `file*.exe` to specify a large category of filenames, which includes filenames like `file01.exe`, `file_new.exe`, `file.exe` and others.

- `?` stands for any single character.

  For example, you can enter `group?_log??.doc` to specify a large category of filenames, which includes filenames like `group1_log01.doc`, `groupA_log19.doc`, `group4_log1a.doc` and others.

All the names excepted from scanning are listed in the box. To remove entries, select them and click **Remove**.

Filtering Attachments by Type

Select **Detect all extensions except for the following** and specify the excepted extensions in order to filter attachments by type. All attachments with extensions other than those specified as exceptions will be detected.

Specify the permitted extensions in the edit field. The extensions must be separated by a semi-colon ";".

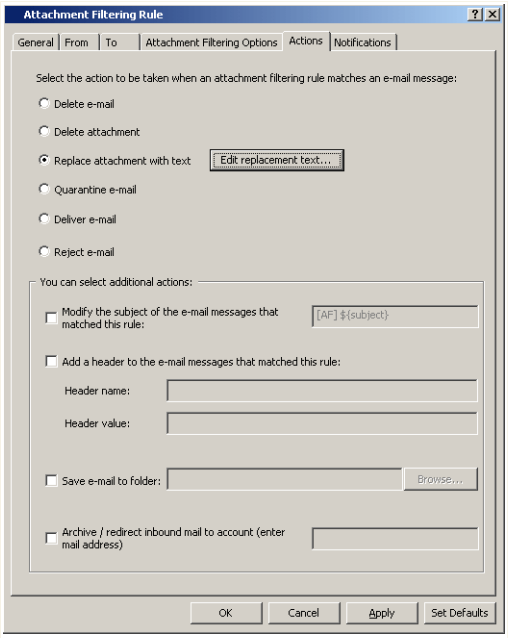
Note
In case of a double extension, only the last extension will be checked.

Filtering Attachments by Size

To detect attachments exceeding a certain size limit, specify the minimum size in the corresponding field. By default, this is set to 0 KB, meaning that no attachment will be detected regardless of its size.

Step 5/6 - Set Actions

Click the **Actions** tab and specify the actions to be taken on the messages containing detected attachments.



Actions

You must choose one of the following actions:

Action	*Description*
Delete e-mail	The message containing the detected attachment is deleted.
Delete attachment	The detected attachment is deleted.
Replace attachment with text	The detected attachment is replaced with a specified text. To specify the text to be delivered instead of the attachment, click **Edit replacement text...**. Provide the text in the edit box that appears and click **OK**.
Quarantine e-mail	The message containing the detected attachment is moved to the quarantine folder.

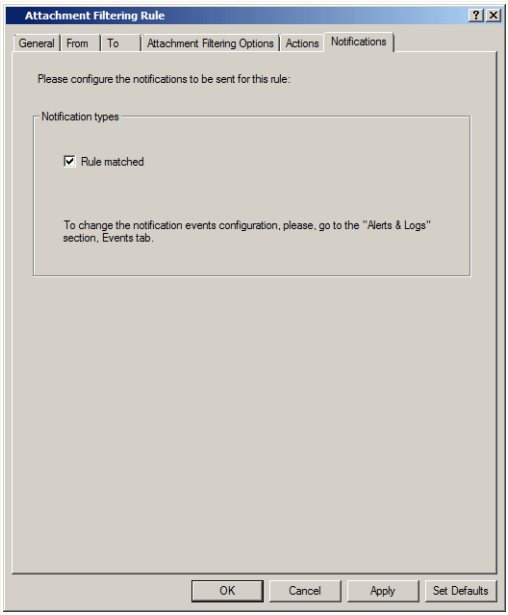
Action	Description
Deliver e-mail	The message containing the detected attachment is delivered in full to its recipients.
Reject e-mail	The detected message is rejected with a 550 SMTP error code.

You can also set additional actions to be taken on the detected messages. The following actions are available:

Action	Description
Modify the subject of the e-mail messages that matched this rule	The subject of the message containing the detected attachments is modified. You can modify the subject pattern. We recommend you to use one of these patterns: • `[AF]${subject}` - to add `[AF]` before the subject. This is the default subject pattern. • `[AF]${subject}[AF]` - to add `[AF]` before and after the subject. • `[AF]` - to replace the subject with `[AF]`.
Add a header to the e-mail messages that matched this rule	An e-mail header is added to the message containing the detected attachment. Provide the header name and value in the corresponding fields.
Save e-mail to folder	The detected message is saved to a specified folder. To specify the folder, click **Browse**, locate it and then click **OK**.
Archive / redirect to account	The detected message is archived to a specified account. Provide the e-mail archive address in the field next to this option. A Bcc containing the address will be added to the detected message.

Step 6/6 - Configure Notifications

Click the **Notifications** tab and specify whether to issue notifications or not when attachments match the rule.



Notifications

Select **Rule matched** to issue notifications when attachments match the rule.

Note

The corresponding event in the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Click **OK** to save the changes and close the configuration window.

15. Update

New viruses and spyware are found and identified every day. This is why it is very important to keep BitDefender up to date with the latest signatures. By default, BitDefender automatically checks for updates every hour.

Updates can be classified in the following ways:

- **Antivirus updates** - as new threats appear, the files containing virus and spyware signatures, as well as the antivirus engine, are updated to ensure permanent up-to-date protection against them.
- **Antispam updates** - new rules are added to the NeuNet (heuristic) and Pre-trained Bayesian filters, new links are added to the URL filter database and new images are added to the Image filter. This helps increase the effectiveness of the Antispam engine.
- Product updates - when a new product version is released, new features and scan techniques are introduced to the effect of improving the product's performance.

Moreover, from the administrator's intervention viewpoint, we may take into account:

- Automatic update - BitDefender automatically contacts the update server in order to check if an update was released. If there are available updates, BitDefender is updated automatically.

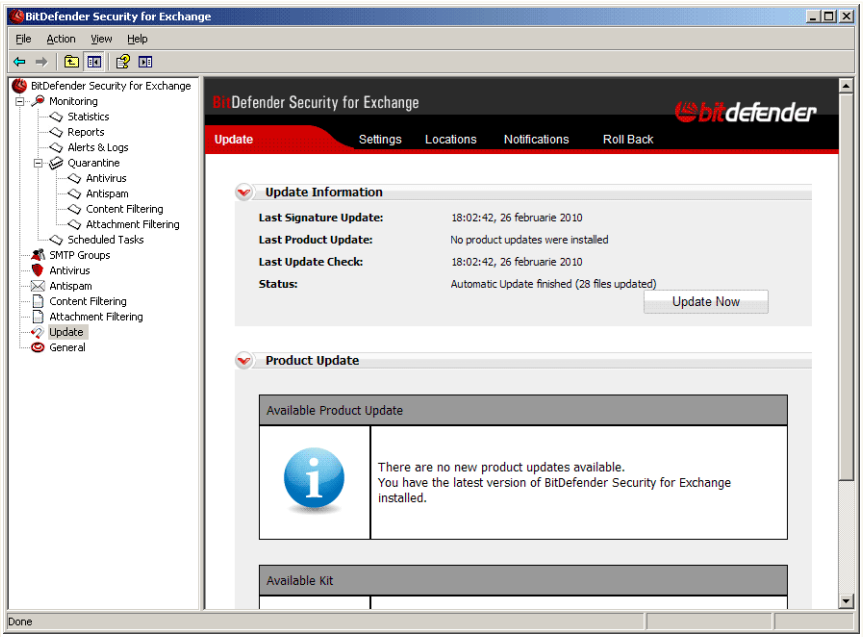
  Note

  In order not to interfere with the server's operation, product updates are not automatically installed. Go to the Product Update section periodically to see if there are any product updates available and to install them.

  The automatic update can also be done anytime you want by clicking **Update now** from the Update section or by creating a scheduled update task.
- Manual update - you must download and install the latest virus and spyware signatures manually.

15.1. Update

To find out information on the update status and if product updates are available, click **Update** in the tree menu and then the **Update** tab.



Update

If you want to update BitDefender immediately, just click **Update Now**. The Update module will check for updates at the specified update locations. If new malware signatures or scanning engine updates are detected, BitDefender will automatically download and install them.

15.1.1. Update Information

In the **Update Information** box, you can see the update status and when the last update check and update were performed.

15.1.2. Product Update

The product updates are different from the signature updates. Their function is to deliver bug fixes and new features to the product.

There are two types of updates for the product:

- **product updates (patches)** - these are files that bring improvements to the current product; they are usually smaller size updates that do not require a new version of the product to be delivered.
- **version updates** - these are installation packages of a new released version of the product.

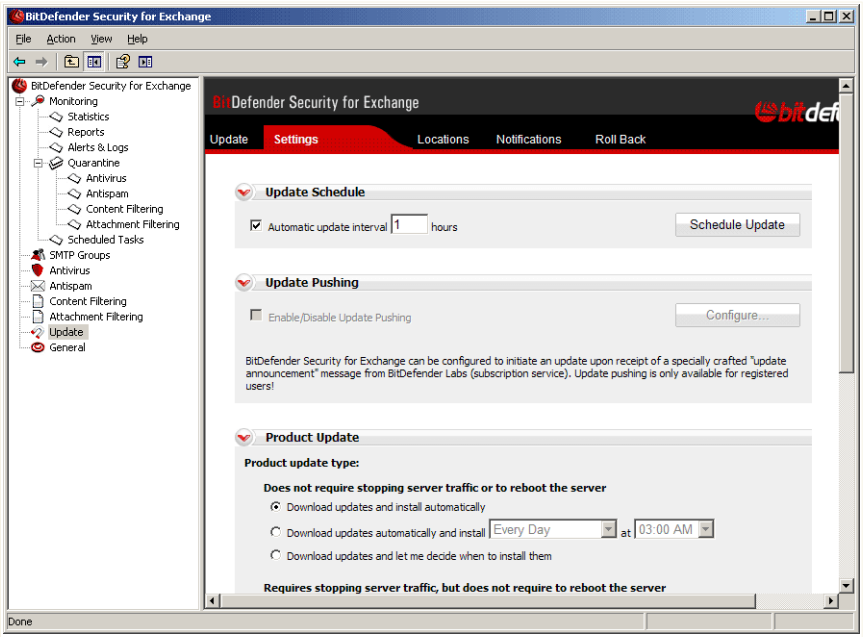
Note
Patches and newer product versions are not automatically installed because they might require a system restart. We advise you to install the latest version of product updates or product version.

When a new patch is available, it is downloaded on the local computer and information about it is displayed. You can then choose if you want to install it immediately or schedule it for a later date.

When a newer version of BitDefender Security for Exchange is available, you will see information about that version. Also, you will be provided with a link to the web page where you can download the installation package from. Click the respective link and download and install the new version.

15.2. Update Settings

To configure the update frequency and the update settings, click **Update** in the tree menu and then the **Settings** tab.



Update Settings

15.2.1. Configuring Update Schedule

There are two ways to update BitDefender Security for Exchange on a regular basis:

- **Using the automatic update.** The automatic update feature allows updating BitDefender automatically, on a regular basis, without the administrator's intervention. By default, BitDefender checks for updates at the specified update locations, every hour. If new malware signatures or scanning engine updates are detected, BitDefender will automatically download and install them.

Important
Keep automatic update enabled in order to be protected against the latest threats.

To change the frequency BitDefender checks for updates, follow these steps:

1. Type the number of hours between two consecutive checks for updates in the **Automatic update interval** field.
2. Click **Apply** to save the changes.

To disable automatic update, follow these steps:

1. Clear the check box corresponding to **Automatic update interval**.
2. Click **Apply** to save the changes.

- **Using a scheduled update task.** Scheduled update tasks allow automatically updating the BitDefender malware signatures and scanning engines according to a convenient schedule. Click **Schedule Update** to create a scheduled update task. For more information, please refer to "*Update Tasks*" (p. 86).

Note
Scheduled update tasks will not de-activate automatic update so that the update locations will be checked for new updates on a regular basis.

15.2.2. Using Update Pushing

Update Pushing is a feature that is available only when the product is registered. This feature allows customers to benefit from "Update Announcement Messages". These alerts are sent to the Update Pushing mailing list by the BitDefender Lab. The mailing list is composed of mail addresses that have been submitted by the customers on the BitDefender website. The "Update Announcement Messages" include special elements which trigger the update process when the message is scanned by the product. Therefore, it is mandatory that the mail address submitted by the customer is a mail address protected by BitDefender.

To enable Update Pushing, check **Enable/Disable Update Pushing**. If you do not want to use this service, clear the corresponding check box.

To subscribe to the mailing list, click **Configure**.

15.2.3. Configuring Product Updates

Installing product updates regularly is essential to the security of your server. Depending on the level of interference with the server, there are three types of product updates:

- product updates that do not require stopping server traffic or to reboot the server
- product updates that require stopping server traffic, but do not require to reboot the server
- product updates that require to reboot the server

To configure automatic downloads and installation for each type of product update, select one of the following options:

- **Download updates and install automatically**

  Select this option and BitDefender will automatically download and install product updates. This is the recommended choice for product updates that do not require stopping server traffic or a server reboot.

- **Download updates automatically and install... at...**

  Select this option if you want BitDefender to install available updates at certain times. Select from the corresponding drop-down lists the date (day and time) when you want this to happen.

  This way you can configure BitDefender to perform product updates at times when it is least likely for interferences to occur with server activity (during night time, for example).

- **Download updates and let me decide when to install them**

  Select this option if you want BitDefender to automatically download product updates, but let you decide when to install them. This is the recommended choice for product updates that require stopping server traffic or a server reboot.

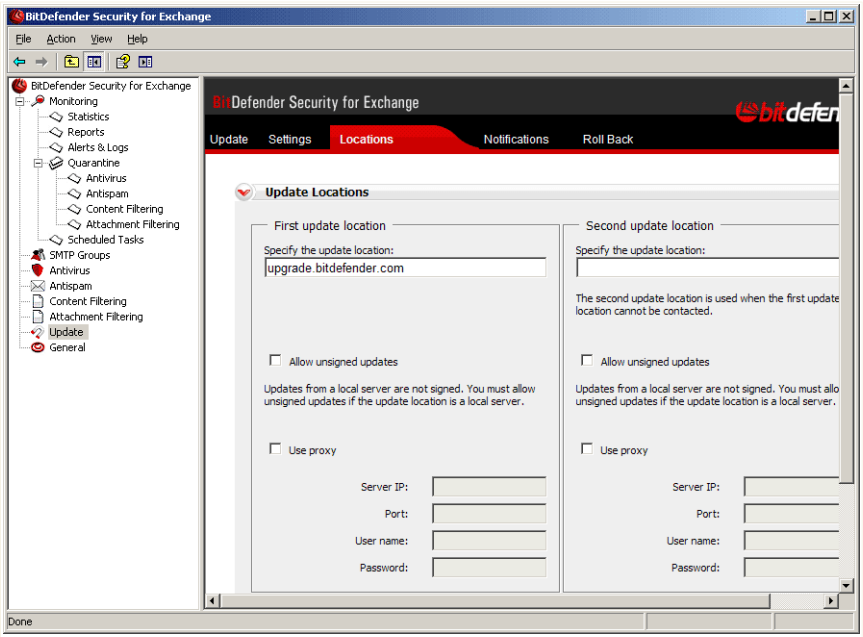
To disable automatic product updates, select the **No automatic product updates** check box.

Note
Your server will be more vulnerable unless you install updates regularly.

Click **Apply** to save the changes.

15.3. Update Locations

To set the update locations, click **Update** in the tree menu and then the **Locations** tab.



Update Locations

BitDefender can update from the local network, over the Internet, directly or through a proxy server.

For more reliable and faster updates, you can configure two update locations: a **First update location** and a **Second update location**. Both require the configuration of the following options:

- **Update location** - type the address of the update server. By default, the primary update location is: `upgrade.bitdefender.com`.

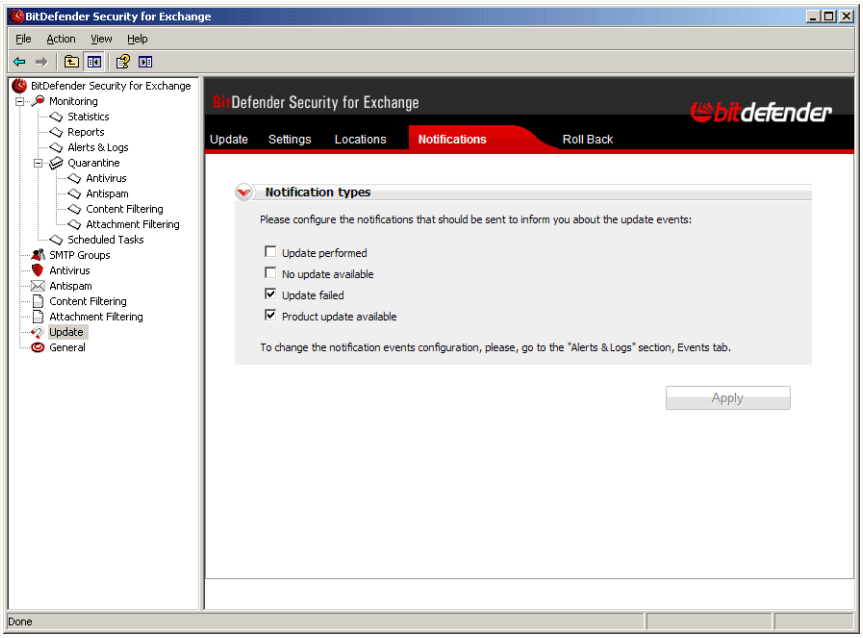
Note
If you are connected to a local network that has BitDefender virus signatures placed locally, you can change the location of the updates here.

- **Allow unsigned updates** - select this option to allow updates from a local server to be installed.
- **Use proxy** - select this option if the company uses a proxy server. The following settings must be specified:
  - **Server IP** - type the IP of the proxy server.
  - **Port** - type the port BitDefender uses to connect to the proxy server.
  - **User name** - type a user name recognized by the proxy.
  - **Password** - type the valid password of the previously specified user.

Click **Apply** to save the changes.

15.4. Update Notifications

Click **Update** in the tree menu and then the **Notifications** tab to enter this section.



Update Notifications

This is where you can specify the update events for which notifications should be issued.

Select the update events for which to issue notifications:

- **Update performed** - when an update was performed.
- **No update available** - when no update is available.
- **Update failed** - when an error occurred during an update and the update failed.
- **Product update available** - when a product update is available.

Note

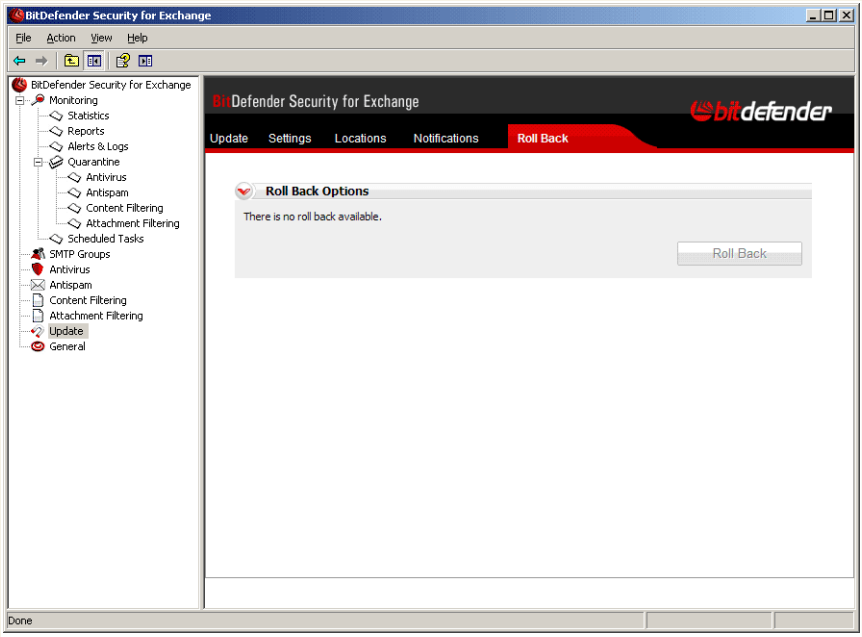
The corresponding events from the Events section must be enabled and properly configured. For more information, please refer to "*Configuring Events*" (p. 70).

Click **Apply** to save the changes.

15.5. Update Roll Back

If you have performed a product update since first installing BitDefender, you can always revert to the previous product version using the Rollback feature. This feature is very useful in case the product starts behaving unexpectedly.

To see if there is any rollback available, click **Update** in the tree menu and then the **Roll Back** tab.



Update Rollback

If a rollback is available, the current product version and the version you can roll back to will be displayed. Click **Roll Back** and confirm your choice by clicking **Yes** in the confirmation window to perform the rollback action.

After a rollback is performed, the version currently in use and the previous version will be displayed. You can use the provided link to update back to the newer version.

15.6. Manual Update

This method allows installing the latest virus and spyware signatures. To install a patch or a product upgrade of the latest version, go to the Product Update section.

Important
Use the manual update when the automatic update cannot be performed or when the computer is not connected to the Internet.

Manual update is performed using a zip archive, `cumulative.zip`, which contains the updates of the scanning engines and virus and spyware signatures.

`cumulative.zip` is released every week on Monday and it includes all the virus and spyware definitions and scan engines updates up to the release date.

Note
The download locations, on FTP and HTTP, are:

- ftp://ftp.bitdefender.com/pub/updates/update_is_90/cumulative.zip
- http://download.bitdefender.com/updates/update_is_90/cumulative.zip

Steps to be followed:

1. **Download the update file.** Please download the cumulative.zip and save it somewhere on your disk when prompted.
2. **Stop antivirus protection.** Open the management console, click **Antivirus** in the tree menu, clear the check box next to **Enable real-time antivirus scanning** and click **Apply**.
3. **Open Services.** Follow the path: **Start** → **Control Panel** → **Administrative Tools** → **Services**.
4. **Stop BitDefender Antivirus Scanning Service.** Right-click BitDefender Antivirus Scanning Service and select **Stop**. The following services should also stop: BitDefender Exchange Connector, BitDefender Mail Scanning Service and BitDefender File Scanning Service. If this does not happen, stop these services one by one.
5. **Copy the update files.** Go to `?:\Program Files\BitDefender\BitDefender for Windows Servers Services\BitDefender Threat Scanner\` and locate the most recent `Engines` folder (the word "Engines" will be followed by a

date stamp in the folder name). Extract the content of the archive in the `Plugins` folder and accept overwriting existing files.

6. **Start BitDefender Antivirus Scanning Service.** Right-click BitDefender Antivirus Scanning Service and select **Start**.
7. **Start BitDefender File Scanning Service.** Right-click BitDefender File Scanning Service and select **Start**.
8. **Start BitDefender Mail Scanning Service.** Right-click BitDefender Mail Scanning Service and select **Start**.
9. **Start BitDefender Exchange Connector Service.** Right-click BitDefender Exchange Connector Service and select **Start**.
10. **Start antivirus protection.** Open the management console, click **Antivirus** in the tree menu, check **Enable real-time antivirus scanning** and click **Apply**.

16. General

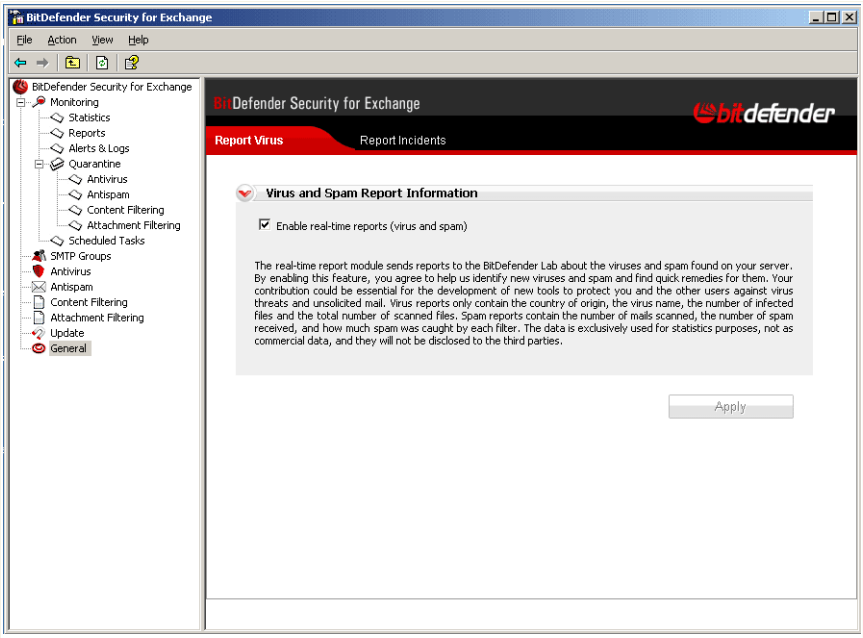
The General snap-in allows configuring BitDefender to send the BitDefender Lab reports regarding the viruses found on the server and the incidents that occurred during product operation.

16.1. Report Virus

Real-time Virus Reporting (RTVR) allows sending reports about the viruses and spam found on your server to the BitDefender Lab in order to help us identify new viruses and spam and find quick remedies for them. Your contribution could be essential for developing new tools to protect you and other users against virus threats.

The reports will not contain any personally identifiable data, such as your name, IP address or others. The virus information supplied will contain only the name of the country, the virus name, the number of infected files and the total number of scanned files. Spam information consists of the number of mails scanned, the number of spam received and how much spam was caught by each filter. The reports themselves are used only for statistic purposes and will never be used as commercial data or disclosed to third parties.

To configure Real-time Virus Reporting, click **General** in the tree menu and then the **Report Virus** tab.


BitDefender Security for Exchange
File Action View Help
BitDefender Security for Exchange
Monitoring
Statistics
Reports
Alerts & Logs
Quarantine
Antivirus
Antispam
Content Filtering
Attachment Filtering
Scheduled Tasks
SMTP Groups
Antivirus
Antispam
Content Filtering
Attachment Filtering
Update
General
BitDefender Security for Exchange
bitdefender
Report Virus
Report Incidents
Virus and Spam Report Information
Enable real-time reports (virus and spam)
The real-time report module sends reports to the BitDefender Lab about the viruses and spam found on your server. By enabling this feature, you agree to help us identify new viruses and spam and find quick remedies for them. Your contribution could be essential for the development of new tools to protect you and the other users against virus threats and unsolicited mail. Virus reports only contain the country of origin, the virus name, the number of infected files and the total number of scanned files. Spam reports contain the number of mails scanned, the number of spam received, and how much spam was caught by each filter. The data is exclusively used for statistics purposes, not as commercial data, and they will not be disclosed to the third parties.
Apply

Report Virus

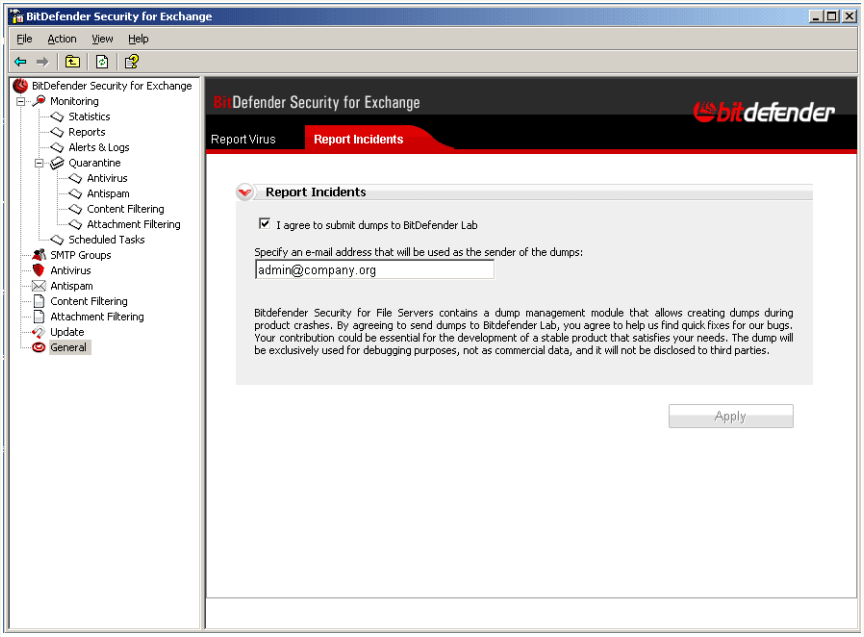
Real-time Virus Reporting is disabled by default. To activate it, follow these steps:

1. Select **Enable real-time virus reports**.
2. Click **Apply** to save the changes.

16.2. Report Incidents

BitDefender Security for Exchange contains an incident management module that allows creating incident reports during product crashes. By agreeing to send the incident reports to the BitDefender Lab, you agree to help us find quick fixes for our bugs. You could make a major contribution to the development of a stable product that satisfies your needs. The reports will only be used for debugging purposes. They will never be used as commercial data or disclosed to third parties.

To configure the incident management module, click **General** in the tree menu and then the **Report Incidents** tab.


BitDefender Security for Exchange
File Action View Help
BitDefender Security for Exchange
Monitoring
Statistics
Reports
Alerts & Logs
Quarantine
Antivirus
Antispam
Content Filtering
Attachment Filtering
Scheduled Tasks
SMTP Groups
Antivirus
Antispam
Content Filtering
Attachment Filtering
Update
General
BitDefender Security for Exchange
bitdefender
Report Virus
Report Incidents
Report Incidents
I agree to submit dumps to BitDefender Lab
Specify an e-mail address that will be used as the sender of the dumps:
admin@company.org
Bitdefender Security for File Servers contains a dump management module that allows creating dumps during product crashes. By agreeing to send dumps to Bitdefender Lab, you agree to help us find quick fixes for our bugs. Your contribution could be essential for the development of a stable product that satisfies your needs. The dump will be exclusively used for debugging purposes, not as commercial data, and it will not be disclosed to third parties.
Apply

Report Incidents

By default, the reports created automatically during product crashes are not sent to the BitDefender Lab. To configure BitDefender to send incident reports to the BitDefender Lab, follow these steps:

1. Select **I agree to submit incident reports to the BitDefender Lab**.
2. Specify your e-mail address.
3. Click **Apply** to save the changes.

Testing BitDefender

17. Antivirus Test

You can verify that the BitDefender Antivirus component works properly by the help of a special test file, known as the *EICAR Standard Anti-virus Test* file. EICAR stands for the *European Institute of Computer Anti-virus Research*. This is a dummy file, detected by antivirus products.

The file can be created using any text editor, provided the file is saved in standard MS-DOS ASCII format and is 68 bytes long. It might also be 70 bytes if the editor puts a CR/LF at the end.

The file must contain the following single line:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Copy this line and save the file with any name and `.COM` extension, for example `EICAR.COM`. BitDefender must treat this file as an infected one.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

Note

The reason we do not include the file in the package is that we want to avoid generating any false alarms for those who use BitDefender or any other virus scanner. You can keep the `EICAR.COM` in a safe place and periodically test the server protection.

You can visit the EICAR website at http://eicar.com, read the documentation and download the file from one of the locations on the following web page: http://eicar.com/anti_virus_test_file.htm.

18. Antispam Test

You can verify that the BitDefender Antispam component is correctly installed and works properly by the help of a special test, known as *GTUBE*. GTUBE stands for the *Generic Test for Unsolicited Bulk Email*.

The test consists of entering the following 68-byte string, as one line, in the body of the email:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

When scanning the email, BitDefender must tag it as spam.

You can visit the GTUBE website at http://gtube.net/, read the documentation and download the sample RFC-822 format email from the locations on the web page.

Troubleshooting and Getting Help

19. BitDefender Configuration Repair Tool

If you have problems with BitDefender Security for Exchange, you can use the BitDefender Configuration Repair Tool to restore the last known good configuration. The BitDefender Configuration Repair Tool backs the configuration file up every hour so that you can restore it if needed. This tool can be successfully used to fix a corrupt configuration file issue, which may occur in extreme situations such as a forced system shutdown caused by a blackout.

To restore the last known good version of the configuration file, follow these steps:

1. Open the BitDefender Configuration Repair Tool using this path from the Windows start menu: **Start → Programs → BitDefender Security for Windows Servers → BitDefender Configuration Repair Tool**.

BitDefender Configuration Repair Tool
BitDefender Security for Windows Servers
bitdefender
BitDefender Configuration Repair Tool helps you restore your last known good configurations of your BitDefender Security for Windows Servers products. All the new settings made after the last moment the configuration files were saved will be lost. You should use this tool only when your current configuration file is corrupted.
Press "Restore" to begin restoring your configuration files, or "Exit" to close this dialog and keep your current settings.
Restore
Cancel

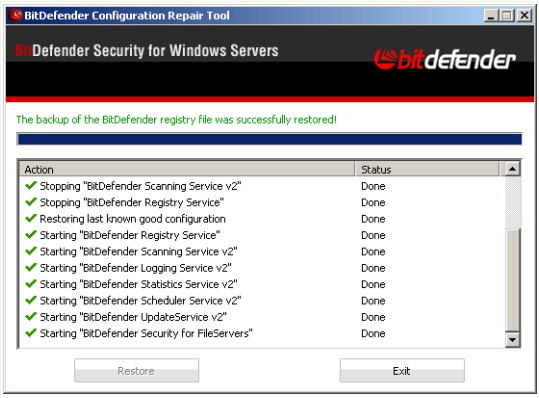
BitDefender Configuration Repair Tool

2. Click **Restore** to begin restoring the backup copy of the configuration file.
3. Wait until the BitDefender Configuration Repair Tool completes the restoration process.

Repairing Configuration

The window displays the status of the restoration process. First, the BitDefender Configuration Repair Tool stops the services belonging to the BitDefender Security for Windows Servers products installed on the system (services belonging to Microsoft applications may also be stopped; for example, Microsoft Exchange Transport, if BitDefender Security for Exchange is installed). Then, the BitDefender Configuration Repair Tool replaces the corrupt configuration file with the backup file (an older working copy of the configuration file). Finally, the BitDefender Configuration Repair Tool restarts the processes previously stopped.

4. The BitDefender Configuration Repair Tool informs you when the backup copy of the configuration file has been successfully restored.


BitDefender Configuration Repair Tool
BitDefender Security for Windows Servers
bitdefender
The backup of the BitDefender registry file was successfully restored!
Action
Status
Stopping "BitDefender Scanning Service v2" Done
Stopping "BitDefender Registry Service" Done
Restoring last known good configuration Done
Starting "BitDefender Registry Service" Done
Starting "BitDefender Scanning Service v2" Done
Starting "BitDefender Logging Service v2" Done
Starting "BitDefender Statistics Service v2" Done
Starting "BitDefender Scheduler Service v2" Done
Starting "BitDefender UpdateService v2" Done
Starting "BitDefender Security for FileServers" Done
Restore
Exit

Finish

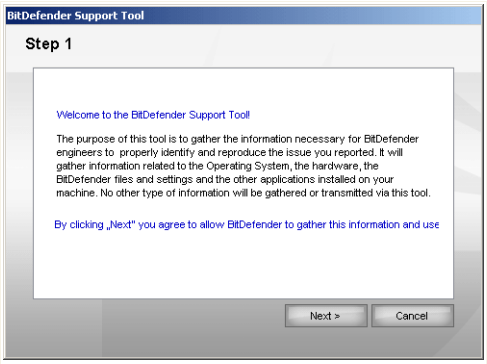
Click **Exit** to close the window.

20. BitDefender Support Tool

The BitDefender Support Tool creates a zip archive of files required by our support technicians to troubleshoot BitDefender Security for Exchange.

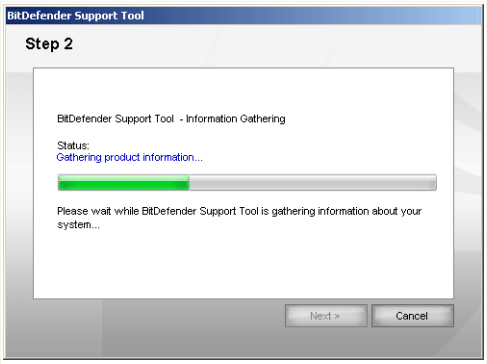
To use the Support Tool, follow these steps:

1. Open the BitDefender Support Tool using this path from the Windows start menu: **Start → All Programs → BitDefender Security for Windows Servers → BitDefender Support Tool**.


BitDefender Support Tool
Step 1
Welcome to the BitDefender Support Tool!
The purpose of this tool is to gather the information necessary for BitDefender engineers to properly identify and reproduce the issue you reported. It will gather information related to the Operating System, the hardware, the BitDefender files and settings and the other applications installed on your machine. No other type of information will be gathered or transmitted via this tool.
By clicking „Next" you agree to allow BitDefender to gather this information and use
Next >
Cancel

BitDefender Support Tool

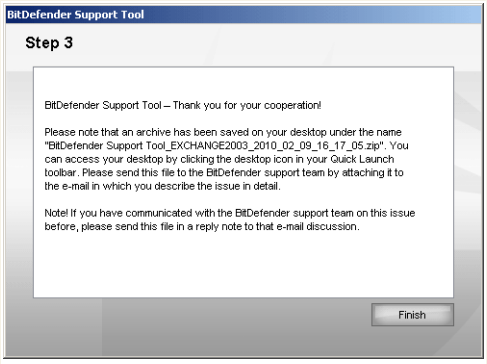
2. Click **Next**.
3. Wait until the Support Tool finishes gathering information.



Gathering Information

The Support Tool gathers product information, information related to other applications installed on the machine and the software and hardware configuration.

4. The Support Tool informs you when the process has completed.


BitDefender Support Tool
Step 3
BitDefender Support Tool – Thank you for your cooperation!
Please note that an archive has been saved on your desktop under the name "BitDefender Support Tool_EXCHANGE2003_2010_02_09_16_17_05.zip". You can access your desktop by clicking the desktop icon in your Quick Launch toolbar. Please send this file to the BitDefender support team by attaching it to the e-mail in which you describe the issue in detail.
Note! If you have communicated with the BitDefender support team on this issue before, please send this file in a reply note to that e-mail discussion.
Finish

Finish

The name of the zip archive that has been created on your desktop is displayed in this window. Click **Finish** to close the window.

You can send the zip archive together with your request for support in order to reduce the time needed to resolve the query.

21. Support

With BitDefender, dedication to saving customers' time and money by providing the most advanced products at the fairest prices has always been a top priority. Moreover, we believe that a successful business is based on good communication and commitment to excellence in customer support.

You are welcome to ask for support at any time. Our customer care representatives will provide you with all the assistance you need.

21.1. Asking for Help

You can ask for help via the BitDefender Web Self-Service or via the telephone. The BitDefender Web Self-Service assists you with solutions to BitDefender-related issues and provides means to contact BitDefender Customer Care. The BitDefender Web Self-Service addresses and the technical support phone numbers are provided in section "*Contact Information*" (p. 226).

To ask for help via the BitDefender Web Self-Service, follow these steps:

1. Go to http://kb.bitdefender.com and access the Business section. This is where you can find the BitDefender Knowledge Base for the BitDefender business products. The BitDefender Knowledge Base hosts numerous articles that contain solutions to BitDefender-related issues.
2. Select your product from the list.
3. Search the BitDefender Knowledge Base for articles that may provide a solution to your problem.
4. Please read the article most relevant to your problem and try the proposed solution.
5. If this solution does not solve your problem, use the link in the article to contact BitDefender Customer Care. It is recommended that you first login to your BitDefender account and then contact the BitDefender support representatives by e-mail, chat or phone.

21.2. BitDefender Knowledge Base

The BitDefender Knowledge Base is an online repository of information about the BitDefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the BitDefender support

and development teams, along with more general articles about virus prevention, the management of BitDefender solutions with detailed explanations, and many other articles.

The BitDefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing BitDefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from BitDefender clients eventually find their way into the BitDefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The BitDefender Knowledge Base is available any time at http://kb.bitdefender.com.

21.3. Contact Information

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

21.3.1. Web Addresses

Sales department: sales@bitdefender.com
Web self-service: http://kb.bitdefender.com
Documentation: documentation@bitdefender.com
Partner Program: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Media Relations: pr@bitdefender.com
Job Opportunities: jobs@bitdefender.com
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Product web site: http://www.bitdefender.com
Product ftp archives: ftp://ftp.bitdefender.com/pub
Local distributors: http://www.bitdefender.com/partner_list

21.3.2. BitDefender Offices

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

North America

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Phone (sales&technical support): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Web Self-Service: http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: vertrieb@bitdefender.de
Website: http://www.bitdefender.de
Web Self-Service: http://www.bitdefender.de/site/KnowledgeBase/showMain/2/

UK and Ireland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
UK
Phone (sales&technical support): +44 (0) 8451-305096
E-mail: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Web Self-Service: http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

Spain and Latin America

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª
08006 Barcelona
España

Fax: +34 932179128
Phone (office&sales): +34 902190765
Phone (technical support): +34 935026910
Sales: comercial@bitdefender.es
Website: http://www.bitdefender.es
Web Self-Service: http://www.bitdefender.es/site/KnowledgeBase/showMain/2/

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Web Self-Service: http://www.bitdefender.ro/site/KnowledgeBase/showMain/2/

EMEA and APAC Business Unit

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Romania
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.com
Website: http://www.bitdefender.com
Web Self-Service: http://www.bitdefender.com/site/KnowledgeBase/showMain/2/